SECRECY AND SERVICE-LOYALTY IN THE AUSTRALIAN DEFENCE FORCE

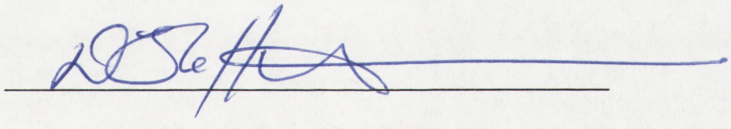
UNDERSTANDING THE SOCIAL PSYCHOLOGY OF PROBLEMATIC NON-DISCLOSURE

DEREK JEAMES BOPPING

A thesis submitted for the degree of Doctor of Philosophy
of the Australian National University
July 2004

DECLARATION

The research reported in this thesis is my own
and has not been submitted for a higher degree
at any other institution.



Derek Jeames Bopping

ACKNOWLEDGEMENTS

Without the support of the Department of Defence and the Defence Science and Technology Organisation I would not have been able to undertake this PhD so it is only appropriate that I acknowledge that support at the outset.

In addition to this support I have been fortunate to have been associated with a number of individuals within DSTO who have played a significant role in helping me and the research along the way. First, Jennie Clothier was not only instrumental in providing me with the opportunity in the first place but her belief in my capacity as a researcher strengthened my resolve during many of the difficult times – many thanks Jennie. I am also very grateful for the patience and support I have received from Leoni Warne during the process.

Many thanks to Craig McGarty for his enthusiasm and dedication to my supervision. I have learned a great deal over the last few years and will miss being under your 'supervision wing'. Additionally, thanks to Mike Smithson who too has provided a great deal of guidance and assistance, encouraging me to think outside the (psychological) square. Thanks also to Kate Reynolds for her ongoing interest and support.

I would also like to thank the technical and administrative staff for their support and friendship over my ANU years so thanks to Kate, Jen, Caroline, Shane, Ricardo, Girish, Trina and Alan, Graham and Greg.

My life at the ANU has been made immensely enjoyable because of the company of James Schuurmans-Stekhoven, Jamie Swann and John Beale over the past few years. 'Stekkie' deserves special mention for his on-going statistical support!

My life at DSTO has also been enriched by the friendship and support I have received from Gordon Martin, Martin Burke, John O'Neill, Paul Prekop, Glen Coomber, Hugh

Barkley, Gary Bulluss, Irena Ali, Abdel El-Sakka, Ed Kruzins, Richard Davis and Brett Biddington.

Much love and many thanks to Mum, Dad, Brendan, Reggie and Carl for their support over the years. It would be remiss of me not to also mention the support I have received from the Veenstra family during this period. In particular Con and Ginno have played a vital role in both keeping my chin up and my head down at the same time – thank you.

Words cannot express how thankful I am for the love and support I have received from my wonderful friend and partner Kris Veenstra. It has been your love and support that has enabled me to grow in so many ways and to believe in myself throughout this time. It is because of you that I see so much more of the world. So all my love, and thank you. I must thank "Jackaga" and "Pussaga" for their unconditional love also!

Last but not least to all those ADF personnel who diligently completed questionnaires at my behest, thanks…

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF DEFENCE ACRONYMS

ADF	Australian Defence Force
ADO	Australian Defence Organisation
AFHQ	Air Force Headquarters
AHQ	Army Headquarters
ARA	Australian Regular Army
CDF	Chief of Defence Force
CSS	Capability Systems Staff
DJFHQ	Deployable Joint Force Headquarters
DMO	Defence Materiel Organization
DSTO	Defence Science and Technology Organisation
KSS	Knowledge Systems Staff
LHQ	Land Headquarters
MHQ	Maritime Headquarters
NCW	Network Centric Warfare
NHQ	Navy Headquarters
RAAF	Royal Australian Air Force
RAN	Royal Australian Navy

ABSTRACT

In the wake of the terrorist attacks of September 11, 2001, the extent to which classified (i.e., officially secret) information is shared within and between organizational groupings has emerged as a matter of great importance. This thesis examines the social psychological processes underlying problematic non-disclosure of classified information in the context of the Australian Defence Force (ADF). In doing so, it provides a psychological account of why ADF personnel might be reluctant to disclose classified information to one another when doing so could be detrimental to the organization as a whole.

The thesis contains four theoretical chapters which address: (1) our current understanding of how classified information comes to be known and not known by ADF personnel (Chapter 2); (2) the contribution that psychology has made in understanding the factors affecting disclosure behaviour (Chapter 3); (3) the social identity perspective, which incorporates both social identity theory and self-categorization theory (Chapter 5); and, (4) the contribution of psychology toward understanding decision-making under risk (Chapter 7). Guided by the analyses in those chapters and insights provided by related sociological literature, two factors emerge as being important to disclosure outcomes, those of Service affiliation and perceived risk. These factors then provide the foundation for the empirical program.

Five studies are reported in the thesis, in addition to a pilot study and some qualitative data gathered by way of interviews with ADF personnel. The issue of whether ADF personnel can be expected to breach official rules in order to avert problematic outcomes associated with the concealment of classified information is examined in the pilot study and Study 1. The role of Service identity with respect to problematic non-disclosure of classified information in the ADF is examined in Studies 2 and 3. Finally, Studies 4 and 5 test a hypothesis of problematic non-disclosure which affirm the centrality of perceived risk in disclosure outcomes, the so-called guardedness hypothesis.

The results of these studies allow us to draw conclusions about the factors likely to contribute to problematic non-disclosure of classified information in the context of the ADF. In Chapter 9, the implications of the work are discussed, some limitations and future directions are outlined, and a final comment about the broader significance of the thesis is made.

CHAPTER 1

INTRODUCTION AND OVERVIEW OF THE THESIS

The issue examined in the thesis

It is now well known that in the months prior to the terrorist attacks of September 11, 2001, the agencies of the United States 'Intelligence Community' had amassed a considerable amount of information pointing to a planned attack on the American mainland (United States House Committee, 2002). Yet, despite the fact that many of these agencies cross-detailed people to each other, the extent to which this information was shared between them was minimal. Instead, information relating to the terrorists' plans (e.g., meetings held, visas granted, pilot training conducted, etc.) was kept largely within the boundaries of the agency that 'owned' it. According to members of the Intelligence Community, the flow of information across agency boundaries had long been impeded by a complex, thorny, and largely informal phenomenon which they had colloquially termed "the Wall" (United States House Committee, 2002, p. 363).

The breakdown of the US intelligence system in relation to the events of September 11, 2001 is arguably the most significant organizational failure in recent history. This particular organizational failure can be seen as an example of a broader phenomenon that could be termed *problematic non-disclosure*. Disclosure is the communication of restricted information (Corcoran & Spencer, 2000; Steele, 1975). Hence, the term problematic non-disclosure refers to situations where concealed and often officially secret information is not communicated and this 'non-communication' results in negative organizational and/or societal outcomes. One need not look far back in history to find other instances of problematic non-disclosure. In 1991 for example, the U.S. Secretary of Defense cancelled a major U.S. Navy project to build the A-12 aircraft after it fell nearly two years behind schedule and $1 billion dollars over budget. Amongst other things, the costly demise of the A-12 was blamed on excessive secrecy between stakeholder groups (Montgomery, 1991). More recently, the Columbia Accident Investigation Board (CAIB) concluded that one cause of the loss of the Space Shuttle *Challenger* and its seven crew was that NASA has

developed a culture of ineffective communication where problems were left unreported and concerns unexpressed (CAIB, 2003).

Of course, problematic non-disclosure of officially secret information within and between organizational groupings need not constitute an organizational fiasco as is illustrated by these cases. In the Australian Defence Force (ADF) for example, officially secret information must be routinely and appropriately disclosed amongst the three Services, that is, the Royal Australian Navy (RAN), the Royal Australian Air Force (RAAF) and the Australian Regular Army (ARA). Any reluctance on the part of ADF personnel to disclose officially secret information, say, that relating to problems with the readiness or capability of their Service, would also be a form of problematic non-disclosure. While it would not likely attract the kind of attention bestowed on those responsible for the A-12 debacle or the *Columbia* disaster, this form of problematic non-disclosure would represent a particularly troubling issue for the ADF. In short, it would signal a breakdown in cooperation between the elements of the ADF, one that could potentially undermine the organization's ability protect and defend Australia's interests.

Why might people who ostensibly share a common organizational purpose fail to disclose valuable information to each other, despite knowing that non-disclosure may court negative outcomes, even disaster? Traditionally, the answer given to this question is one informed by a view of organizations as 'rational' systems (see Scott, 1992; Thompson, 1967). Problematic non-disclosure, traditional reasoning goes, is a largely aberrant event that can be avoided if organizational rules and procedures are better designed, defined, and followed (Erickson, 1979). This reasoning paves the way for the introduction of structural solutions designed to minimize or indeed, eliminate problematic non-disclosure. Yet, it side-steps a more fundamental and critically important issue, one that ultimately determines the efficacy of such solutions. This issue relates to the *psychological* factors that give rise to problematic non-disclosure in the first place.

The broad aim of this thesis is to investigate these factors. To that end, two factors are examined. The first is *group affiliation*, that is, people's sense of belonging to various organizational groups and categories. As implied above, the

particular organizational groups of concern in this thesis are the Services to which ADF personnel belong, that is, the RAN, the RAAF and the ARA. The second is *risk*, that is, people's perception that the consequences of their decision-making include the prospect of loss (Smithson, 1994). Guided by the results of an exploratory study, these factors are manipulated in a series of scenario-based experimental studies involving ADF personnel that focus on the potential disclosure of *classified* (i.e., officially secret) information. In the following sections, the background to the research problem is outlined and a brief review is made of the psychology of disclosure behaviour. The chapter then concludes with an overview of the thesis chapters.

Background to the research problem

Over the past two decades, organizations across Australia and indeed the world over, have sought to undergo a transformation. Government bureaucracies, finance companies, and developers of information-technology to name but a few, have attempted to step out of the mould they occupied during the 1980's to become fully-fledged 'knowledge organizations'. To support the transformation, an entire industry devoted to organizational change has emerged, offering technologies and ideologies believed to be essential for effective knowledge management (see Lawson & Samson, 2003). Despite this activity, the 'knowledge organization' remains a fuzzy concept, as does for that matter, the notion of 'knowledge management' (Warne, Agostino, Ali, Pascoe, & Bopping, 2003). However, a number of simple ideas can be distilled from the literature. For one, the knowledge organization is said to leverage better organizational outcomes by exploiting the tacit knowledge or 'organizational wisdom' of members, rather than just their knowledge of organizational rules and procedures (Warne, Agostino et al., 2003). Further, knowledge organizations are seen to be those that exhibit high levels of trust between members which underpins the free and appropriate sharing of knowledge and information (Chandra Sekhar & Anjaiah, 1995). In the words of one industry participant, the knowledge organization is one with a "knowledge-sharing culture" (Smith & McKeen, 2003, p. 5).

These ideas are not entirely new. For some years, organizational theorists and practitioners have espoused the benefits of harnessing both tacit knowledge (Wagner

& Sternberg, 1987) and trust (Kramer & Tyler, 1996; Mayer, Davis, & Schoorman, 1995). Indeed, for decades it has been argued that the success of all organizational endeavours depends on the effective sharing of information and knowledge, whether it be between individuals, groups, divisions or departments (Katz & Kahn, 1966; March & Simon, 1958). However, the ideas generated by contemporary discourse on knowledge management do retain a particular potency in respect to certain types of organizations. In these organizations, a 'sharing culture' is not just desirable for the sake of increased productivity, profit or workplace harmony, but because the consequences of not having one can be catastrophic. Clearly, the exemplar in this respect is the modern military organization. Military personnel such as those of the ADF must now plan for, conduct, and manage a range of activities both on and off the battlefield, most of which are ill-defined, opened-ended, and demand a high degree of cooperation and information-sharing between people of different Services (Dorman, Smith & Uttley, 1998). The backdrop to most (if not all) of these activities is the risk of placing people's lives and a nation's security in jeopardy, and of wasting staggering amounts of money, time and effort. If a sharing culture must be achieved anywhere, it is in the modern military organization.

Over the past decade or so, defence policy makers in various countries have produced a number of strategic-level 'frameworks' that speak to the idea of securing such a culture. The most salient of these at the present time is the doctrine of *Network Centric Warfare* (NCW) which has held the centre-stage of military policy in Australia, the United States and Great Britain for a number of years now (see Wilson, 2004). According to NCW, increases in computer processing power and networked communications will be exploited over the next decade to provide military and defence personnel with a 'shared awareness' of situations, both inside and outside the theatre of operations (Warne, Ali, Bopping, Hart, & Pascoe 2003; see also Wilson, 2004). The vast amount of discussion that NCW has generated has provided answers to many important questions about securing this shared awareness, such as what information-technologies are likely to be required and what structure the 'network-centric' defence organization should take (Warne, Ali et al., 2003). However, despite such progress, relatively little is said about other factors that may facilitate or indeed underpin the emergence of a shared awareness in the military context (Warne, Ali et al., 2003). Instead, there is a sense of inevitability about the issue of free and

appropriate transfer of information once the correct organizational structures and information technologies are devised and put in place. Put another way, there is an assumption amongst many defence policy makers that 'if you build it, they will share'.

The basis of this assumption, at least in large part, is the idea that other *more fundamental* organizational processes will take care of information-sharing, ensuring it is as free and appropriate as is required. This idea is grounded in the correct belief that the information of major relevance to military activities, and indeed that which forms the core of NCW, is likely to be *classified* (i.e., officially secret) information. Specifically, classified information is "information in any form or of any nature, which requires protection in the interests of national security" (Australian Department of Defence, 1998, Glossary, p. 4) and this protection takes the form of a set of rules that govern its transfer between not only ADF personnel but those of the broader Australian Defence Organization (ADO)[1]. As a result, there is a normative framework already in place regarding the sharing of classified information between defence personnel and this constitutes our 'commonsense view' of how certain individuals come to know (or not know) certain pieces of classified information. In other words, we intuitively believe that classified information flows along the contours of official policy and because official policy is inherently objective and 'rational' (Scott, 1992), it flows are always sufficient and in the 'right' direction. For the personnel concerned, this belief provides a sense of certainty and predictability for activities that are very often performed against a backdrop of uncertainty and risk.

Yet this idea has critical limits. For one, the official rules shed no light on why classified information may sometimes *not* flow along the contours of official policy or why the decrees of official policy may not always match what defence personnel themselves think is 'right'. More fundamentally however, the idea that classified information flows according to the objective prescriptions of official rules must be questioned. Classified information is, by definition, *concealed* information and therefore the extent to which it is disseminated stems from individuals and groups

1. The Australian Defence Organisation includes all personnel of the Australian Defence Force and all civilian members of the Australian Public Service employed by the Department of Defence.

making disclosure decisions. Like all decision-making, the disclosure and non-disclosure of classified information is grounded in psychological processes no matter how 'objective' or impartial the decision-making criteria appear to be. Indeed, it is because the disclosure of classified information is a psychologically mediated activity that we can explain why disclosure outcomes do not always accord with what is envisaged by official policy. Thus, the nature of any sharing culture as it relates to classified information is underpinned by the psychological factors affecting individual's disclosure decisions.

As outlined earlier, the terrorist attacks of September 11, 2001 have brought this deeper psychological issue into sharp relief. On this occasion, the attacks were enabled not because classified information was shared when official policy said it should not be, but because it *was not shared* when the letter and the spirit of official policy said it should be. Furthermore, this particularly catastrophic instance of problematic non-disclosure is merely the most prominent amongst many others, eroding the idea that such episodes are merely aberrant events or random results in an imperfect system. Indeed, problematic non-disclosure of classified information enjoys an even longer history than these cases suggest (e.g., Lowry, 1972). In recent years, its most salient form has been the phenomenon known as *overclassification* (see Washington Post, 2001). The core idea here is that in order to impede or restrict another's access to classified information, the source of the information will classify it to a degree well above that which is adequate and appropriate. There is a psychology that underpins overclassification and problematic non-disclosure more generally, yet systematic efforts to investigate the factors influencing this psychology have not been made.

In contrast, and as alluded to above, the standard response to problematic non-disclosure of classified information has tended to be structural in nature. In the wake of September 11 for example, the U.S. Government established the Department of Homeland Security (DHS), an organization charged with unifying the vast network of organizations that play a role in ensuring the internal security of that country, including the FBI and the CIA (United States Department of Homeland Security, 2004; see also United States Department of Justice, 2003). In Australia, similar moves are afoot, with intentions to establish an organization similar to the DHS, and a

number of calls have been made to improve the procedures and processes for sharing sensitive information amongst Australia's defence agencies, particularly those with an intelligence-related function. Despite the good intentions of these responses, they also risk an opportunity lost. As implied earlier, there is a mild suggestion within such responses that problematic non-disclosure of classified information will be solved if formal rules and procedures are better defined, designed, and followed (Erickson, 1979). Such a suggestion arguably underplays the psychological processes involved in the phenomenon.

Contemporary defence science in Australia is also yet to adequately address the issue of problematic non-disclosure of classified information. In general, defence science has tended to steer away from asking personnel when and why they might not do 'as they are supposed to' particularly when classified information is the issue at hand (Bok, 1984). Of course there are some exceptions here such as those attempts to explain why personnel might leak classified information (e.g., Sarbin, Carney & Eoyang, 1994). There have also been many internal studies of ADF personnel which have focused, in part or in full, on the extent to which classified information is disclosed (see Warne, Agostino et al., 2003 for a review) and these have helped identify instances of adequate and inadequate disclosure. However, their descriptive nature preclude them from identifying the factors that actually *cause* disclosure outcomes it to be adequate or inadequate. What is required is an examination of the phenomenon from a psychological perspective. The aim of this thesis to take a modest first step toward fulfilling that requirement.

A brief overview of the psychology of disclosure

While the factors affecting non-disclosure of classified information remain under-theorized and under-researched, the psychological study of other forms of disclosure behaviour has spanned many decades. The result has been a broad an in-depth understanding of the psychological processes likely to be involved in the revelation or withholding of concealed information from one person to another. Despite recent attempts to provide an integrative analysis of disclosure behaviour (see Corcoran & Spencer, 2000), the psychological study of disclosure and non-disclosure must be seen as a heterogeneous field of enquiry, spanning various phenomena

including secrecy and secret societies, self-disclosure, confidentiality, and whistle-blowing. The work is divergent in its disciplinary background, core concerns, and theoretical underpinnings. All in all, this makes disclosure behaviour a field that is *phenomenon-driven* field rather than *theory-driven* (see Smithson & Foddy, 1999). However, and at the risk of oversimplification, two broad traditions can be identified.

In the first tradition, disclosure and non-disclosure are viewed as behaviours driven by group affiliation. The central idea here is that people's group affiliations provide a kind of psychological foundation to facilitate either (i) their willingness to disclose to other group members, and/or (ii) their willingness to withhold information from 'outsiders'. A number of mechanisms have been advanced in this respect with most converging on the idea that group affiliation provides information about the trustworthiness and shared goals of the potential recipient. Thus, the primary hypothesis is that people's disclosures and non-disclosures follow the contours of their perceived group affiliations. A good example is provided by Hargie, Dickson, and Rainey (2002) who found that the amount of personal information disclosed between youths in Northern Ireland was related to whether the recipient was of the same religion. Another body of work in this area examines, not so much how existing group affiliations influence one's disclosures and non-disclosures, but how people may use disclosure and non-disclosure to establish or reinforce a sense of group affiliation. This is well illustrated by work examining 'disclosure reciprocity' (e.g., Moon, 2000) where disclosing is thought to constitute a display of trustworthiness and the desire to establish a relationship. This idea is also central to theory and research on 'secret societies' (Bellman, 1981; B. H. Erickson, 1981; MacKenzie, 1967; Simmel, 1906) where non-disclosure constitutes a group norm that defines who is an insider and who is not.

In the second tradition, disclosure and non-disclosure are argued to be driven by perceptions of risk. The main idea here is that the expected consequences of disclosing and not disclosing shape one's decision-making. Again, a subdivision is evident according to whether the expected consequences are seen to drive the individual to either disclose or not disclose. With respect to the former, it is held that as the perceived risks associated with continued concealment of the information increase, the more likely people will be to breach the norms or rules that mandate its

concealment and decide to disclose. This notion dominates work which has addressed breaches of confidentiality (e.g., Lindenthal, Amaranto, Jordan, and Wepman; 1984) and is also evident in the literature regarding whistle-blowing (e.g., Rothschild & Miethe, 1999). With respect to the latter, it is thought that disclosing information is inherently risky and that as fears relating to the consequences of disclosing increase, the more likely people are to withhold the information. This idea dominates analyses of self-disclosure (i.e., the disclosure of personal information; Hendrick, 1987; Jourard, 1971) and is discussed in sociological analyses of secrecy. Despite the fact that it is rarely conceived of in this way, the underlying theme running through this literature is an assumption that people make decisions about whether or not to disclose based on their preferences, much in the spirit of subjective expected utility theory (Savage, 1954; von Neumann & Morgenstern, 1944). Changes in the degree of disclosure behaviour or the nature of one's disclosure decision are seen to be due to variations in the utility of disclosing relative to not disclosing.

As stated above, the aim of this thesis is to examine how both group affiliation and risk are likely to affect the disclosure of classified information by ADF personnel, and that the groups of interest are the Services of the ADF. In so doing, we hope to gain some insight into the psychological factors underpinning the problematic non-disclosure of classified information in this particular context. In the following section a summary of the individual thesis chapters is presented.

Overview of the chapters

The aim of Chapter 2 is to set the scene for a psychological analysis of the disclosure of classified information in the ADF. To this end, the chapter begins by reviewing of the official rules that govern access to classified information in this organization. These rules constitute the formal organizational blueprint *vis-à-vis* the disclosure of classified information and hence also underpin our 'commonsense' view of how classified information comes to be disclosed and not disclosed amongst ADF personnel. The main premise here is that classified information comes to be known by those who have a 'need to know' pending the possession of an adequate level security clearance, and not known by those who do not fulfil either or both of these conditions. It will be argued that this formal model does not provide an adequate

explanatory framework for understanding actual disclosure outcomes. As part of this argument, the fundamental assumption that another's 'need to know' can be impartially determined is challenged and the need to understand the disclosure and non-disclosure of classified information as a *psychologically mediated* activity is articulated.

As alluded to above, the discipline of psychology has long had an interest in the factors affecting the extent to which people disclose information. To the extent that this interest constitutes a field of psychological enquiry (see Wagner & Berger, 1985), it is one that is 'phenomenon-driven' rather than 'theory-driven'. Specifically, the psychological study of disclosure and non-disclosure comprises attempts to clarify the psychological processes underlying various social phenomena, primarily self-disclosure, confidentiality, whistle-blowing, and other forms of secrecy. This literature is reviewed in Chapter 3 with an eye for how it might contribute toward gaining an understanding of the psychological factors involved in the problematic non-disclosure of classified information in the ADF. Attention converges on two broad factors, the notions of *risk* and *group affiliation*.

The first empirical component of the thesis is presented in Chapter 4. The aim of this chapter is to gain an insight into whether ADF personnel will breach official rules to avert problematic non-disclosure and if so, when and for whom? In other words, we seek to determine when and for whom the prospect of problematic non-disclosure will 'override' the formal rules mandating non-disclosure of classified information and, by implication, when it will not. Two studies are presented in this chapter. The first study constitutes a pilot involving a sample of civilian defence scientists while the second (Study 1) is a refinement of the pilot involving a larger sample of ADF officers drawn from various strategic-level organizations within the ADF. While interesting differences emerge between these populations, the results of both studies point to the importance of risk and Service affiliation as factors shaping disclosure outcomes in the domain of national security. More importantly, the results of Study 1 suggest that social identification processes may be the psychological mediator of Service affiliation in this respect.

We examine the idea that social identification processes might underpin disclosure and non-disclosure outcomes more closely in Chapter 5 with a review of the social identity perspective. This perspective is comprised of social identity theory (Tajfel & Turner, 1979; see also Tajfel & Turner, 1986) and self-categorization theory (Turner, 1985; Turner, Hogg, Oakes, Reicher, & Wetherell, 1987; see also Turner, 1982). Over the past few years, the social identity perspective has made significant contributions in explaining the psychological processes involved in issues of importance to organizations notably trust, communication, and cooperation. These contributions are reviewed with an eye to how social identification processes might therefore be involved in non-disclosure of classified information in the ADF. Two preliminary hypotheses are formulated. The first is derived from the idea that group affiliation can be threatened by the presence of other groups and lead to a process of competition for positive ingroup distinctiveness (Tajfel, 1978; Tajfel & Turner, 1979). The second is drawn from the idea that prosocial perceptions and behaviours follow the contours of salient ingroup-outgroup memberships (Turner et al., 1987).

Both these hypotheses receive empirical attention in Chapter 6 in separate scenario-based experimental studies. Unlike Study 1 which focuses on an entrustment relationship between the source and the potential discloser of classified information and the conditions where it will likely be breached, these studies focus more fully on the relationship between the potential discloser and potential recipient of classified information. The chapter begins by investigating the extent to which the achievement and/or maintenance of positive Service distinctiveness is related to disclosure outcomes (Study 2). This hypothesis is set in context by the ongoing debate in modern military and defence circles concerning the ideology of 'Jointness' and the extent to which it constitutes an identity threat to Service identity. Following this, we examine the extent to which disclosure outcomes follow the contours of salient ingroup-outgroup memberships (Study 3). Here, we explore whether the extent to which ADF personnel are willing to disclose classified information can be varied by changing the criterion for ingroup membership.

The concept of risk has enjoyed a long history in the theoretical literature, primarily within the field of decision-making. In Chapter 7, we review the theoretical perspectives relating to decision-making under risk, confining our focus to three

particularly influential theories that have held sway at one time or another. These are subjective expected utility theory (Savage, 1954; von Neumann & Morgenstern, 1944); prospect theory (Kahneman & Tversky, 1979); and regret-theory (Bell, 1982; Loomes & Sugden, 1982). On the basis of these theories, we cast the potential discloser of classified information as a decision-maker under risk. This demands we answer a more fundamental question *vis-à-vis* problematic non-disclosure of classified information in the ADF: risk of what? To help answer this question, we turn to the sociological literature on secrecy. The chapter concludes with an articulation of what comes to be termed *the guardedness hypothesis* of problematic non-disclosure.

The guardedness hypothesis is tested in Chapter 8 in the final two empirical studies. First, in Study 5, our aim is to empirically validate the argument that the disclosure of classified information both within and across Service boundaries is perceived by ADF personnel to be associated with many classes of risk. In this study, we also seek to gain an insight into how one's level of confidence toward these risks is affects their confidence about being able to determine another's 'need to know'. In Study 6, we employ a final scenario-based experimental design to test the causal nature of these associations. Specifically, and building upon ideas presented in the field of organizational decision-making, we manipulate levels of risk by varying the extent to which ADF personnel perceive they have control over how the disclosed information may be used. In the final chapter, Chapter 9, we provide an integration of the work conducted in the thesis. To this end, the empirical work is drawn together to offer a social-psychological account of problematic non-disclosure of classified information in the ADF.

CHAPTER 2

CAN DISCLOSURE BE TREATED AS A RATIONAL NORMATIVE ACT?

Introduction

In the previous chapter, the research issue was defined and an overview of the thesis and its chapters was presented. In doing so, the question guiding this thesis was posed: why might ADF personnel not disclose classified information to one another, despite knowing that non-disclosure could have negative, even disastrous outcomes? This kind of question has been asked many times in the wake of major organizational failures, most recently the failure of the US intelligence community to forestall the September 11 terrorist attacks. Traditionally, the question has been answered in a way which assumes that complex organizations can avoid the perils of problematic non-disclosure if formal rules and procedures are better designed, defined and followed, and if better use is made of information technologies designed to facilitate information-sharing. Little attention however, has been paid to the psychological factors that might underpin problematic non-disclosure, save the occasional reference to vague constructs such as "personal factors" and "organizational culture" (United States House Committee, 2002).

The aim of this chapter is to set the scene for a psychological analysis of disclosure and non-disclosure in the context of the ADF. More specifically, the scene is to be set with reference to the disclosure and non-disclosure of *officially secret* (i.e., 'classified') information amongst members of this organization. At first blush, arguing for a psychological analysis to be brought to bear on the disclosure of classified information in the ADF may seem misplaced. Access to classified information in this organization (and indeed all modern defence forces) is governed by a set of official rules and it is these rules that constitute our commonsense view of the mechanism underpinning disclosure outcomes, rather than human psychological processes. However, this commonsense view is inadequate insofar as providing an explanatory framework for understanding disclosure outcomes. It ignores the fact that all organizational decision-making including the decision to disclose or withhold classified information is mediated psychologically. It is only through a recognition of

this that we can begin to explain why disclosure outcomes do not always accord with the letter and/or the spirit of what is prescribed by an organization's formal rules.

In the wake of September 11, 2001 and other debates that have issues of "who knew what?" and "why wasn't it passed on?" as their core theme (e.g., Ellsberg, 2003; Marr & Wilkinson, 2003), interest in the organizational control of information and knowledge has enjoyed a recent revival. Against this broad backdrop, the chapter begins with a review of the official rules and procedures governing access to classified information in the ADF, what we term 'the formal model'. This idea that organizational outcomes can be predicted on the basis of a set of official rules and procedures is central to the rational approach to organizational analysis. Therefore, a brief and critical review of this approach follows, before our attention turns more specifically to the limitations of the formal model. It is argued that despite overtones of objectivity and rationality, the operation of the formal model rests on psychological processes of judgement and attribution. As a result, problematic non-disclosure in ADF must be examined through a psychological lens.

The formal model

In an increasingly competitive global economy, the need for organizations to protect their most valuable information is paramount. No longer prepared to rely solely on the goodwill of their employees, many organizations have set in place 'information management' policies designed to ensure that the 'right' people (and *only* the right people) come to know certain information at certain times (see Gunasekaran, Khalil, & Rahman, 2003). For many organizations, these policies are better described as systems of 'information control' (Wilsnack, 1980). They include explicit regulations which define what information needs to be protected and from whom, how it must (and must not) be shared, and the punishments that await those whose behaviour breaks the rules. Rather than resting on the implicit expectation that trade secrets and the like must not be disclosed to 'outsiders', these policies are often legally binding and forbid any such discussions taking place (Bok, 1984).

Organizational control over 'who knows what' arguably reaches its peak in government bureaucracies. Within the past decade or two, there has been a steady

stream of literature devoted to the practice of information control by governments, either in general (e.g., Aftergood, 2000; Demac, 1984; Doyle, 2000; Moynihan, 1998; Stevenson, 1980) or written in response to specific and usually disastrous events (e.g., Marr & Wilkinson, 2003). Without doubt, the exemplar of information control by government is the modern defence organization, particularly as it relates to matters of intelligence. Interestingly however, defence organizations have been spared much of the negative commentary that has pervaded accounts of information control in other spheres of government, particularly within the executive (Bok, 1984; for a recent exception, see Aftergood, 2000). One of the primary reasons for this is that information control in defence and military organizations is perceived by the general population to be a legitimate form of government secrecy (Bok, 1984). It need hardly be explained why information relating to a nation's defence arrangements must be controlled and restricted from the view of 'outsiders'. Control over this type of information is fundamental to ensuring a nation's security and minimizing the grave risks that are inevitably faced by a nation's military personnel in 'operational' contexts.

In Australia, the disclosure of classified information is governed by a set of formal rules that apply not only to ADF personnel, but to all personnel employed across the wider ADO. This set of rules is underpinned by the notion of 'national security'. In Australia, national security is formally defined as:-

> The protection of the Commonwealth and the people of Australia from any actual or threatened action, by any agency, organization or individual, foreign or otherwise, which are designed to influence, intimidate, or undermine the defence of the nation, or its international relations. (Australian Department of Defence, 1998, Glossary, p.11).

More specifically, national security refers to the protection of Australia's interests from a range of potentially harmful activities. These may include espionage (i.e., spying), politically motivated violence, attacks on Australia's defence system, the undermining of its defence plans and operations, and damage to its international relations (Australian Attorney-General's Department, 2000). It is this notion that is core to the definition of 'classified' information:-

> Official information or matter in any form or of any nature that requires protection against unauthorised disclosure in the interests of national security, and that has been so designated (Australian Department of Defence, 1998, Glossary, p. 4)[2].

Strictly speaking, classified information is more correctly known as *national security information* which can be distinguished from *non-national security information* (Australian Attorney-General's Department, 2000). Where unauthorised disclosure of national security information is thought to present a risk to national security, unauthorized disclosure of non-national security information is associated with "lesser" harm, such as that to Australian individuals, groups, commercial entities and the like. The use of the category titles 'national' and 'non-national security information' stems from a confusion that arises from the fact that both types of information undergo a classification process when produced, meaning that both are in a sense 'classified'. However, the term 'classified information' is routinely used to refer to national security information.

The actual process whereby information becomes 'classified' involves the assignment of one of four hierarchically arranged classifications that prescribe the extent to which the information is to be protected. From the lowest to the highest, these classifications are: RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET. Where information that receives a TOP SECRET classification demands the utmost protection, that which receives a RESTRICTED classification requires only some protection by comparison. The particular classification assigned is that which is judged by the information's originator (i.e., the person responsible for preparing the information) to be commensurate with the *degree of damage* to Australia's national security that may result from unauthorised disclosure of the information. Classifications and commensurate degrees of damage to national security are shown in Table 2.1.

---

2. The term "unauthorised disclosure" is defined more fully later in this chapter. At this point, it is sufficient to say that it refers to disclosure of classified information to those who are deemed *by way of official policy* to be inappropriate recipients of such information.

Table 2.1

Information classifications in the Australian Defence Organization

Classification	Unauthorised disclosure could...
RESTRICTED	Possibly be harmful to national security
CONFIDENTIAL	Cause damage to national security
SECRET	Cause serious damage to national security
TOP SECRET	Cause exceptionally grave damage to national security

(Source: Australian Attorney-General's Department, 2000)

According to the official rules, an individual is authorised to access to classified information if they satisfy two criteria. First, the intended recipient must possess an adequate level security clearance. In the Australian Defence Organisation (ADO), a security clearance is an official advice that an individual is considered suitable to have access to classified information up to a specified level (Australian Department of Defence, 1998). An adequate-level clearance is one that is commensurate with, or of a higher level than the information's designated classification. For example, to be eligible to access SECRET information, the intended recipient must hold either a SECRET or a TOP-SECRET clearance. Via this mechanism (amongst others), highly classified information comes to receive greater protection than less classified information since the granting of higher-level security clearances involves significantly more scrutiny of the individual (in the form of background checks and the like) than does the granting of lower-level clearances.

In addition to an adequate level security clearance, authorised access to classified information is dependent upon the intended recipient possessing a 'need to know'. In the ADO, 'need to know' is defined as:

> A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his/her official duties (Australian Department of Defence, 1998, Glossary, p. 11).

The 'need to know' criteria thus restricts the basis for accessing classified information to official necessity. In so doing, it excludes all other circumstantial arguments for gaining access to classified information, regardless of whether the intended recipient possesses an adequate level security clearance. For instance, the condition excludes circumstances where access to classified information would be convenient for the intended recipient, where the intended recipient believes that they may have a need to know the information at a later point in time and so on. Together, the two criteria constitute the primary mechanism through which the ADO (and modern defence organizations generally) seek to limit the disclosure of classified information amongst the personnel to the absolute minimum, that is, to those for whom it is officially necessary.

In summary then, the disclosure of classified information in the ADF context is governed by a set of official rules that apply to all ADO personnel. These are the rules governing access to classified information. They state that the intended recipient must possess both an adequate level security clearance and a 'need to know' in order to have access to classified information. Further, these rules seek to ensure that only appropriate persons access classified information and to prevent inappropriate disclosure of such information, either by accident or by intention (Australian Department of Defence, 1991). The idea that organizational outcomes including decision-making can be predicted on the basis of official rules such as these is central to the rational approach to organizational analysis. Therefore, a brief and critical review of this approach is in order at this point.

Rational organizational analysis: A brief review

The assumption that organizational phenomena can be understood and predicted on the basis of official rules and procedures lies at the heart of the rational approach to organizational analysis (Hall, 1977; Scott, 1992). As implied by Thompson's (1967) quote below, the central tenet of rational analysis is the notion that organizational phenomena, including human behaviour and decision-making, are (or can be) deliberately and objectively planned and executed (Argyris, 1960; Bennis, 1959; Erickson, 1979; Hall, 1977; Thompson, 1967):

> The rational model of an organization results in everything being functional – making a positive, indeed an optimum, contribution to the overall result. All resources are appropriate resources, and their allocation fits a master plan. All action is appropriate action, and its outcomes are predictable. (p. 6).

Consequently, the theoretical and empirical focus of the rational approach is squarely on processes of organizational control (Hall, 1977; Scott, 1992). Dimensions of organizational structure are considered to be the fundamental control mechanisms, circumscribing human behaviour and decision-making so as to ensure that personnel behave in 'calculated ways' (Hall, 1977). Essentially, the perspective sees personnel as instruments that are shaped by rules, roles and regulations, and whose efforts can be channelled directly into accomplishing explicitly articulated goals (Gouldner, 1959; March & Simon, 1958; Scott, 1992). With this 'certainty-oriented' posture, formal organizational structure is regarded as the ultimate determinant of behaviour.

It is widely accepted that Max Weber's (1946) thoughts on bureaucracy provide the theoretical roots of the perspective (Hall, 1977; Haralambos & Heald, 1985; Scott, 1992). According to Weber, the bureaucracy is "rational action in an institutionalised form" (Haralambos & Heald, 1985, p. 280). Weber lists a number of characteristics that, together, comprise the 'ideal-type' bureaucracy. Generally speaking, the following five characteristics are considered to be the core elements (see Haralambos & Heald, 1985; Scott, 1992). First, the bureaucratic mode of administration involves the distribution of regular tasks and activities as official duties. In this way, complex tasks such as providing a system of taxation or planning civil infrastructure are broken down amongst personnel with clearly defined spheres of competence and responsibility. Second, the ideal-type bureaucracy is organized along hierarchical lines and possesses a graded authority structure. Hence, an administrative 'chain of command' is established that orders a system of super- and subordination. Third, bureaucratic administration involves a strict separation of private and official income and property whilst, and fourth, personnel occupying bureaucratic office are selected of the basis of their technical expertise, rather than kinship or inheritance. Finally, and particularly relevant to our interest in the formal model of access to classified information, bureaucratic operations are governed by a consistent (i.e., fixed) set of abstract and impersonal rules.

In all organizations, a system of administration capable of coordinating the activities of elements (e.g., individuals, groups, departments) toward, and in line with prescribed organizational goals is critical. Weber saw bureaucracy as a mode of organization that sought this coordination through having officials perform their duties in accordance with "calculable rules" (Weber, 1946, p. 215), that is, rules and procedures which can be applied in a seemingly impartial or 'computable' way. In the ideal-type bureaucracy, such rules are applied with impersonal formality, or in Weber's words "without regard for persons" (Weber, 1946, p. 215). He saw these rules and their impersonal application as underpinning the technical superiority of bureaucracy over all other modes of human organization - as the reason why only this mode of organization can effectively and indefinitely coordinate the actions of a large number of people toward a common goal:

> [Bureaucracy] develops the more perfectly the more bureaucracy is 'dehumanized', the more completely it succeeds in eliminating from official business love, hatred, and all purely personal, irrational, and emotional elements which escape calculation. This is the specific nature of bureaucracy and it is appraised as its special virtue (Weber, 1946, p.216).

For Weber (1946), the discharge of bureaucratic business according to calculable and impersonal rules secure an objectivity where "rules, means, ends, and a matter-of-factness dominate" (p. 244)[3].

Yet, the rational approach has long been viewed as providing an incomplete and inaccurate framework upon which to understand and predict organizational phenomena (Erickson, 1979; Hall, 1977; March & Simon, 1958). Specifically, it is widely accepted that norms of rationality are incapable of providing absolute standards, and that organizational conduct and social relations which deviate from the formal plan are inevitable (Blau & Scott, 1962; Hall, 1977). Tsoukas (1998) for instance, argues that:

---

[3]. It is important to note that while Weber analysed rational bureaucracy and how it arose, he did not *advocate* this form of human organization.

> Organized contexts cannot rely on calculable rules alone. Weber's linear logic...can be seen at best as a ceteris paribus argument for the development of formal organization. We have seen enough in the last hundred years to make us have serious doubts about whether formal organizations can really function effectively as programmable machines (p. 48)

By ignoring or seeking to eliminate rather than incorporate factors which cannot be controlled or accurately predicted by organizational structure, the rational approach represents what are essentially "organizations without people" (Bennis, 1959. p. 263). The emphasis is on rules and regulations and not actual human behaviour or decision-making. In short, structure is embraced, action is ignored and very little organizational variance is eventually explained (Hall, 1977; Scott, 1992; Thompson, 1967). The upshot is that the rational approach does not contain sufficient specification of the psychological processes underpinning organizational behaviour (Katz & Kahn, 1966). The social and organizational context capable of shaping these processes having been excluded from the analytical framework from the very beginning.

Subsequent theoretical reasoning in organization theory shifted the interpretive framework from the rules and regulations of the formal blueprint to specification of these psychological processes and their contextual determinants (e.g., Katz & Kahn, 1966; March & Simon, 1958, Blau & Scott, 1962). In doing so, it has argued that human action takes place in interactive and open-ended contexts and "is always a local matter...whose features cannot be fully anticipated" (Tsoukas, 2001, p. 9). From this more 'open-systems' perspective, social relations between an organization's personnel are not taken to be 'disembedded' or 'decontextualized' by formal rules and any 'deviance' such as that represented by problematic non-disclosure of classified information is argued to have psychological correlates, reflecting not random but patterned and adaptive responses to "problematic situations" (Thompson, 1967, p. 7). On this note, it would seem pertinent to return to the formal model and offer a more specific critique of its ability to provide an adequate explanatory framework for understanding disclosure outcomes in the ADF.

A critique of the formal model

The formal model outlined at the beginning of this chapter lays down a set of official rules to be employed by ADF personnel in determining whether or not to allow others access to classified information. In doing so, it constitutes our commonsense view of the mechanism underpinning disclosure outcomes in this organizational context. That is, we intuitively feel that classified information comes to be known by those who have a 'need to know' pending they are sufficiently 'cleared', and not known by those who do not satisfy either (or both) of these criteria. This level of understanding may be all that is required when disclosure outcomes accord with the formal organizational blueprint, that is, when there is a general consensus amongst members of the organization that disclosure outcomes reflect what is 'right' according to the formal model. However, and as alluded to in the previous section, we begin to encounter problems with this level of understanding once we move away from ideal outcomes and toward those where there is discord and disagreement as to what is 'right' in this respect, such as cases of problematic non-disclosure.

We can illustrate this using a simple 2 x 2 matrix in which the outcome of a particular disclosure decision (i.e., to disclose or withhold classified information) is matched against the outcome which is 'right' or 'appropriate' according to the formal model (see Figure 2.1). In a given disclosure situation, an individual may decide to either disclose (D) or not disclose (ND) classified information, where the latter option may include other courses of action such as delaying a decision or passing it up the chain of command. Furthermore, in a given disclosure situation, one of these alternatives is the 'appropriate' one according to the prescriptions of the formal model. That is, the formal model would have one disclose (D) or not disclose (ND) the information. Hence, we have four possible disclosure outcomes: (i) *appropriate disclosure* - disclosing when one should; (ii) *inappropriate disclosure* - disclosing when one should not; (iii) *inappropriate non-disclosure* - not disclosing when one should disclose; and (iv) *appropriate non-disclosure* - not disclosing when one should not disclose.

		Actual decision: D	Actual decision: ND
'Appropriate' decision	D	Appropriate disclosure	Inappropriate non-disclosure
	ND	Inappropriate disclosure	Appropriate non-disclosure

Figure 2.1 A basic framework of disclosure outcomes.

An explanation of appropriate disclosure and appropriate non-disclosure can be derived from the formal model in its 'natural' form without any trouble. In the case of the former outcome, one would infer that the intended recipient had a 'need to know' and was sufficiently cleared, whereas in the case of the latter, the intended recipient must not have met one or both of these conditions. To explain inappropriate disclosure (e.g., 'leaks' of classified information) however, additional factors must be introduced. For obvious reasons, military and defence organizations have long been interested in these factors and they are discussed more fully in Chapter 4. Likewise, additional factors are needed to explain inappropriate non-disclosure, what we have termed 'problematic non-disclosure'. Regardless of whether it is problematic or not, the formal model can only explain non-disclosure by inferring the absence of either a 'need to know' or an adequate-level security clearance. Yet, inappropriate non-disclosure *by definition* implies the fulfilment of these conditions. That is, it suggests that the intended recipient had, at the very least, a 'need to know' the information to perform their official duties and would (or *should*, by virtue of this 'need to know') have possessed an adequate-level security clearance. It would be hard to maintain, for instance, that officials from the FBI, CIA, and NSA did not possess a need to know certain information that each other had collected before September 11, 2001.

The problem with the explanatory capacity of the formal model *vis-à-vis* inappropriate (i.e., problematic) non-disclosure stems from a fundamental assumption that underpins the use of formal criteria in organizational decision-making. This assumption is that the formal criteria upon which organizational decisions are made are impartially determinable. That is, the criteria and extent to which they are fulfilled exist as 'states in Nature' that can be accurately determined or 'fixed' at any given point in time. The formal model governing access to classified information appears to have impartially computable or 'rational' properties (Lowry, 1972). Indeed, this is clearly the case with respect to the adequacy of the intended recipient's security clearance - it is either objectively adequate or inadequate for accessing the relevant information. However, things are less clear regarding the impartiality of the second criteria, whether or not the intended recipient has a 'need to know'.

On the surface, another's 'need to know' classified information appears to be an impartially computable criterion. That is, it seems intuitive to see the information as *inherently* necessary or unnecessary for the intended recipient to perform their official duties. However, on closer inspection, the argument that 'need to know' lies within the domain of organizational rationality cannot be maintained. The reason for this is that despite its rational and objective overtones, another's 'need to know' is not an inherent quality of information *per se*. Instead, it is a *psychological process* of perception and judgment as to what another needs so as to achieve certain ends at a given place and time. Indeed, because these processes relate to potential changes in the 'knowledge state' of another person (i.e., how disclosing will change what they know), the determination of 'need to know' constitutes a psychological process *about a psychological process in another*. Hence, the intended recipient's 'need to know' exists not only as a perception in the eye of the custodian of classified information, but also as a judgment and attribution made by latter about the former.

As a psychologically mediated process, the determination of another's 'need to know' is likely to be shaped by forces and factors that shape psychological processes more generally, such as the prevailing social context and social norms (see Turner, 1991; Turner et al., 1987). This 'shaping' of need to know is well illustrated by situations in which one's need to know is contested, that is, circumstances where people disagree as to whether or not a given individual or group has a need to know

certain information. Clearly, if another's 'need to know' were impartially computable, scope for these kinds of disagreement would not exist. Yet such disagreements are evident with respect to the breakdown of the US intelligence community prior to September 11, 2001. For example, intelligence analysts were often denied access to classified information from intelligence collectors. Whereas the analysts perceived themselves to have a 'need to know', collectors often disagreed, not so much because the information did not relate to the analysts' work duties, but because the collectors viewed the analysts as not needing to know *other things* that might be inferred from the information, such as how it was collected and by whom. Of course, these disagreements must be understood in their local context. However, they illustrate a fundamentally important point - that the determination of 'need to know' is far from a rational, normative act and is likely to vary according to the factors which are psychological salient in the mind of the potential discloser of classified information at a given time.

Summary and the way ahead

Our commonsense understanding of how classified information comes to be disclosed across the ADF is founded on norms of rationality. Access to classified information is governed by formal rules assumed to be interpreted and applied with the same objectivity that Weber outlined a century ago. It is further assumed that their applicability and interpretation remains consistent across all contexts. On this basis that we derive an 'official expectation' that the disclosure and non-disclosure of classified information in the ADF follows a gradient that is objectively 'right'. Yet, such ideas are clearly problematic. Official rules like as those outlined above, provide no explanation of when or why disclosure outcomes will not accord with the letter or spirit of official policy. What is needed to understand problematic non-disclosure of classified information is a recognition that disclosure behaviour is a psychologically mediated activity. Just as researchers have sought to bring into play psychological explanations for why military and defence personnel disclose classified information when they should not (see Sarbin et al., 1994), so too must the same attention be brought to bear to help explain why such personnel will not disclose classified information when, at least in the eyes of some, they should. In the chapter that follows, we review the contribution that psychology has made in understanding

human disclosure behaviour in an effort to identify the factors that may be important in this respect.

CHAPTER 3

RISK AND AFFILIATION:

THE PSYCHOLOGY OF DISCLOSURE

Introduction

In Chapter 2, the scene was set for a psychological analysis of disclosure and non-disclosure as it applies to classified information in the ADF. In doing so, it was argued that the official rules governing access to classified information (what we termed the formal model) does not provide an adequate explanatory framework for understanding actual disclosure outcomes. Rather than being the 'rational' output of objectively determinable decision-making criteria, disclosure outcomes are the result of psychologically mediated processes and as such will not always accord with what is envisaged by the organization's formal blueprint. In order to understand the *when* and *why* of problematic non-disclosure, we must view the phenomenon through a psychological lens. The task now is to identify the broad psychological factors that are likely to impact on ADF personnel's decisions to disclose classified information. The aim of this chapter is to review the progress that has already been made *vis-à-vis* the psychology of disclosure phenomena.

There are a number of social phenomena which involve people disclosing information to (or alternatively, concealing it from) one another. Although varying in the extent to which they have attracted empirical and/or theoretical attention from psychologists, the literatures concerning self-disclosure, confidentiality, whistle-blowing, and secrecy are all of relevance here. Compared to the large volume of work dealing with the psychology of self-disclosure, relatively little is known about the factors affecting an individual's willingness to disclose confidential information or to 'blow the whistle'. Nonetheless, each of these literatures is important and in this chapter they are reviewed and their contribution to the current research problem is outlined. We begin by proposing a basic model of disclosure as a *social process*. The purpose of this is twofold. First, such a model will provide a standard backdrop against which each of the four phenomena outlined above can be discussed. Second,

it provides a basic framework against which to discuss the factors that may play a role in determining disclosure outcomes as they relate to classified information in the ADF.

Disclosure as a three-party process: A conceptual model

In proposing a basic model of disclosure behaviour, it is important that it represent those parties capable of influencing disclosure outcomes. To this end, a model of disclosure is proposed in which three parties are represented: (i) the 'potential discloser', (ii) the 'source', and (iii) the 'potential recipient'. The *potential discloser* is, quite simply, the entity who may disclose or not disclose the information of concern. For example, the potential disclosers of interest in this thesis are ADF personnel and the information of concern is classified information. The *source* is the entity who has provided the potential discloser with the information. As will be seen later in the chapter, the nature of the source can vary considerably. For instance, the source may comprise an individual, a group, or an organization and they may have provided the information to the potential discloser either directly or indirectly. The *potential recipient* is the entity to which the potential discloser may or may not disclose the information. Like the source, the characteristics of the potential recipient may vary widely. They too may be an individual, group, or organization who has explicitly requested the information or who is being considered by the potential discloser as a possible target for a 'spontaneous' (i.e., non-requested) disclosure.

Clearly, the potential discloser lies at the heart of the model and this is depicted in Figure 3.1. The unbroken arrow between the source and the potential discloser indicates that the latter has been provided with the information or knowledge by the source. In other words, entrustment or 'first-phase' disclosure has already taken place. The broken arrow between the potential discloser and the potential recipient indicates that the former is yet to disclose the knowledge or information to the latter and may ultimately decide not to do so.

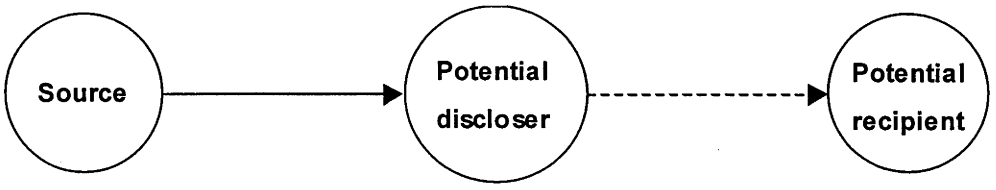


Figure 3.1 A model of disclosure as a three-party process.

In this way, the model represents the potential discloser's decision as part of a broader social process, rather than as a decision confined to an individual in isolation. This 'process perspective' is important in that it allows consideration of factors other than those relating to the characteristics of the potential discloser *per se* (e.g., personality factors). More specifically, situating the potential discloser's decision within a broader social context promotes the idea that disclosure outcomes can be influenced by the relationship that the potential discloser has with both the source and the potential recipient. The relationship that has received the most attention in the psychological literature is that between the potential discloser and the potential recipient as it relates to the phenomenon of *self-disclosure*.

Self-disclosure: The interplay of risk and trust

The term 'self-disclosure' refers to an individual's revelation of personal information (e.g., thoughts, feelings, past experiences) to another or others (Hendrick, 1987; Jourard, 1971). Because self-disclosure relates to the revelation of *personal* information, the 'potential discloser' and the 'source' are one and the same individual. Hence, self-disclosure represents a compression of the three-party process presented above into one involving two parties, as depicted in Figure 3.2.

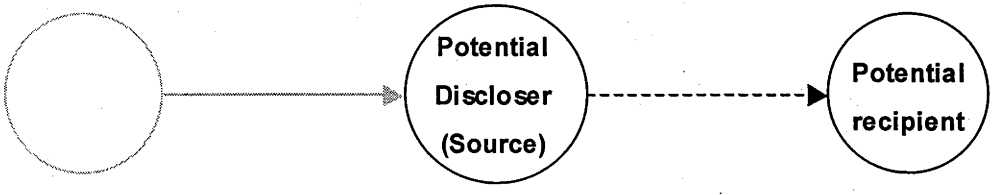


Figure 3.2 Self disclosure as a two-party process.

The self-disclosure literature is vast, spanning work conducted in both clinical (e.g., psychotherapy) and non-clinical (e.g., friendships, family relationships) settings (Yovetich & Drigotas, 1999). In clinical settings, self-disclosure serves to bring information concerning the client's troubles to the fore (Farber, 2003). It is widely agreed that the extent to which a client 'self-discloses' is positively related to constructive therapeutic outcomes and hence self-disclosure is considered a vital element of psychotherapy (Hill, Gelso, & Mohr, 2000; see Farber & Hall, 2002 for a review). In non-clinical settings, self-disclosure is also considered a positive and beneficial process. For instance, the disclosure of personal information is thought to be critical in promoting psychological growth and facilitating one's ability to establish and maintain close and intimate friendships (Derlega, Metts, Petronio, & Margulis, 1993; Hargie et al., 2002; Miller & Boon, 2000).

The importance of self-disclosure for the efficacy of clinical and non-clinical outcomes has meant that the factors affecting people's willingness to self-disclose have attracted considerable research attention. Generally speaking, these factors fall into one of two broad categories: (a) individual difference (i.e., personality) factors, or (b) 'relational' factors. The former category is comprised of a diverse range of personality and individual-differences variables including *attachment style* (Mikulincer & Nachshon, 1991; Pistole, 1993; Vrij; Paterson, Nunkoosing, Soukara, & Oosterwegel, 2003), *locus of control* (Wheeless, Erickson, & Behrens, 1986) and *shame-proneness* (Farber & Hall, 2002). To illustrate, Pistole (1993) found that people with a 'secure' attachment style (i.e., those comfortable with close relationships) were more comfortable with the disclosure of personal information than those with an 'avoidant' or 'anxious/ambivalent' attachment style. Wheeless et al., (1986) on the other hand, found that people with an 'external' locus of control (i.e., a belief that they cannot control the rewards they receive) were more willing to disclose personal information than those with an 'internal' locus of control (i.e., a belief that they can control these rewards).

By way of contrast, the second category is comprised of factors specific to the *relationship* between the potential self-discloser and the potential recipient. One that has attracted a great deal of attention in clinical settings is the 'therapeutic alliance',

that is, the extent to which the client and the therapist share an emotional bond and common goals (Farber, 2003). Generally, as the therapeutic alliance grows 'stronger', clients become more willing to disclose personal information to clinicians (Farber & Hall, 2002). A second relational factor that has attracted a great deal of attention is 'disclosure reciprocity'. The idea here is that an individual's willingness to self-disclose varies according to whether the potential recipient has, or is expected to disclose in return (Hill & Stull, 1982; Moon, 2000). However, discussions of self-disclosure have been dominated by a more general factor, one that is conceived of as both a relational *and* a personality factor. This is the concept of *trust.*

Despite continual debates regarding the meaning of trust (Kramer, 1999; Lewicki & Bunker, 1995), a widely accepted definition proposed by Mayer et al., 1995) defines trust as one's willingness to be vulnerable in some way to another (see also Bigley & Pearce, 1998; Rousseau, Sitkin, Burt, & Camerer, 1998). More specifically, Mayer et al., (1995) define trust as:

> ...the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party (p. 712)

This definition reflects a core assumption held by most trust researchers that *risk* is a necessary precondition for trust (Dasgupta, 1988; Doney, Cannon, & Mullen, 1998; Lewis & Weigert, 1985). The term 'risk' refers to a type of uncertainty that includes the prospect of loss (i.e., hazard or danger; Smithson, 1994), and in the context of trust relates to the uncertainty and vulnerability *vis-à-vis* the actions of the 'trustee' (Doney et al., 1998). Numerous studies have sought to establish trust as an antecedent to self-disclosure by emphasising the fundamental role of risk (Petronio & Bantz, 1991; Vrij, Nunkoosing, Paterson, Oosterwegel, & Soukara, 2002). For example, in disclosing personal information people risk rejection by the recipient of the information, and thereby embarrassment, shame, social isolation and betrayal, if the recipient discloses the information to others (Petronio & Bantz, 1991; see also Petronio, Reeder, Hecht & Mon't Ros-Mendoza, 1996). Because of such risks, the potential discloser's beliefs about the *trustworthiness* of the potential recipient is

considered to be a major factor influencing whether self-disclosure takes place. These ideas can be set against the basic disclosure framework as shown in Figure 3.3.

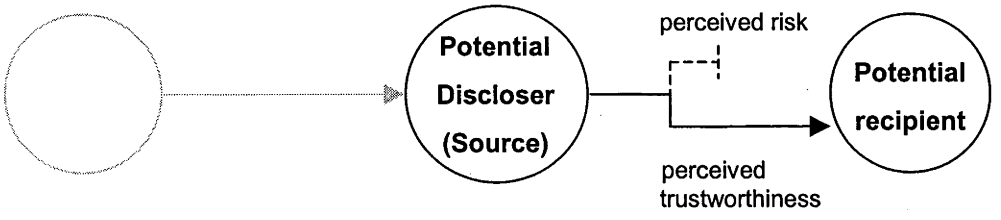


Figure 3.3 Self-disclosure as mediated by perceived risk and trustworthiness

---

As suggested above, trust has been viewed in two ways in discussions of self-disclosure, as either an individual-difference factor or a relational factor. The former conception of trust is known as *generalized trust*, a concept which can be traced back to Rotter (1967). Rotter believed that on the basis of their early experiences, people develop beliefs about the trustworthiness of others and that this generalizes over time into a relatively stable personality trait (Kramer, 1999; Lewicki & Bunker, 1995). At first blush, a direct association between generalized trust and self-disclosure appears intuitive (Wheeless & Grotz, 1977). Indeed, Corcoran (1988) and more recently Steele (1991) offer support for this idea. Corcoran (1988) investigated the extent to which one's willingness to self-disclose correlated with their scores on Rotter's (1967) Interpersonal Trust Scale (ITS), a commonly used measure of generalized trust. Willingness to self-disclose was assessed in terms of one's responses to a number of personal and potentially embarrassing questions. Results showed that those who scored low on the ITS were generally less willing to respond than those who scored highly. Similarly, Steele (1991) found that scores on the ITS correlated positively with self-reports of the amount of self-disclosure to significant others. However, these studies stand against a backdrop of early research in which this relationship failed to materialise. MacDonald, Kessel, and Fuller (1972) for example, compared two measures of generalized trust as predictors of self-disclosure, the ITS and a measure based on participants' choices in a 'Prisoner's Dilemma' matrix, and found that only the latter predicted self-disclosure (see also Cash, Stack and Luna; 1975; McAllister & Kiesler, 1975; Vondracek & Marshall, 1971).

Efforts to link trust and self-disclosure have been more successful when trust is conceptualised as a relational factor, so-called *individualized trust*. Rather than reflecting personality, individualized trust is *relationship specific* trust. That is, it refers to the truster's beliefs about the intentions of a specific trustee (Foubert & Sholley, 1996). Research by Wheeless and Grotz (1977) compared individualized and generalized trust as predictors of various aspects of self-disclosure including (i) the intention to self-disclose, (ii) the amount disclosed, (iii) its honesty and accuracy, and (iv) its 'depth' or intimacy. Participants in this study were asked to think about a specific recipient of personal information (e.g., 'mother', 'father', 'co-worker') and then completed an instrument measuring their level of generalized and individualized trust, and the aspects outlined above. Results indicated that individualized trust was positively related to a many dimensions of self-disclosure, specifically, the conscious intention to disclose, the amount of information disclosed, and its overall depth. In contrast, generalized trust failed to predict any of these dimensions. After replicating this, Wheeless (1978) concluded "the relationship of disclosure and trust is more probably a 'state' rather than a 'trait' phenomenon" (p. 153).

While these findings indicate a positive association between individualized trust and a willingness to disclose personal information, they do so in the context of the laboratory (see also Foubert & Sholley, 1996). Recent research has sought to investigate the impact of trust on self-disclosure in 'real-world' contexts. One of the most frequently examined contexts in this respect is that pertaining to positive HIV diagnoses (Charbonneau, Maheux and Beland, 1999; DeMatteo et al., 2002; Levy et al., 1999; Sauka & Lie, 2000). Again, the risks associated with disclosing this information (e.g., rejection, stigma, prejudice, threats to physical safety, and so on) mean that the perceived trustworthiness of the potential recipient remains a key factor. To this end, Charbonneau et al., (1999) found that one of the main reasons why HIV-positive persons chose not to disclose this information to their dentists was that they considered them to be untrustworthy, that is, they believed there was a risk their dentists would disclose the information to others (see also Sauka & Lie, 2000). A similar theme emerges in work examining the disclosure of other types of sensitive information. For instance, Boon and Miller (1999) found that trust was a key factor in the decision of homosexual men to disclose their homosexuality to their mothers (see also Miller & Boon, 2000; Ponse, 1976), while Petronio et al., (1996) found that

sexually abused children only disclosed information about their abuse to trusted confidants.

Summary and implications

Clearly, the self-disclosure literature is limited in its capacity to provide an understanding of the factors likely to affect the disclosure of classified information. For one, it relates to the revelation of *personal* information rather than officially secret information. Despite the tendency for defence personnel to sometimes claim a sense of "ownership" over officially secret information (United States House Committee, 2002) the two forms of disclosure obviously cannot be equated. Secondly, self-disclosure is process confined to two parties - the potential discloser and the potential recipient - since the former is also the source. Yet, the potential discloser of classified information is not necessarily its source. Defence personnel are frequently provided with classified information by other parties who may be individuals, groups, or other organizations.

Having said that, the work outlined above does offer important psychological points that may arguably apply to the disclosure of classified information in defence organizations and which may have potential in an analysis of problematic non-disclosure in this domain. Specifically, the relationship between risk, trust, and disclosure that is made salient in the self-disclosure literature is also likely to be relevant to disclosure of classified information in defence settings. This is because risk is embedded within the disclosure of classified information just as it is within the disclosure of personal information. In other words, just as the disclosure of personal information entails the prospect of loss, so too may disclosing classified information. In the case of the latter however, the loss may pertain to national security and, at times, the lives of military personnel. Hence, it is reasonable to assume that the perceived trustworthiness of the potential recipient of classified information will be salient in the mind of its potential discloser, particularly when the risk is great. In order to build on this basic hypothesis, it is necessary to turn to literature regarding other disclosure phenomena in which is a separate source of information is present. To that end, we now review those psychological analyses relevant to the operation of *confidentiality*.

Confidentiality: Competing consequences

Confidentiality refers to the ethical and/or legal requirement of some persons (e.g., professionals such as doctors, psychologists, bankers) to respect their client's right to privacy (Bok, 1984; Jacques & Folen, 1998; Taylor & Adelman, 1989). To this end, it comprises a set of principles that mandate non-disclosure of information entrusted by one's clients (e.g., medical and financial records) to third parties, regardless of whether it has been sourced from the client directly or from one's professional colleagues. However, a distinction is made between two types of confidentiality (Watkins, 1989). The first type, *absolute* confidentiality, mandates non-disclosure under all circumstances. The second and more familiar type, *relative* confidentiality, mandates non-disclosure up to a point beyond which the professional is obligated to disclose, that is, to commit a 'breach' of client confidentiality.

Confidentiality is a 'cornerstone' construct in professional contexts (Watkins, 1989). In assuring clients that the information they disclose to professionals will not be disclosed further, it signifies a trust between the two parties which promotes the client's sharing of information and intention to remain in the relationship (Hook & Cleveland, 1999; Watkins, 1989). Ford, Millstein, Halpern-Felsher, and Irwin (1997) recently reported empirical support for this idea in a study that examined the impact of physicians assurances about confidentiality on adolescents' willingness of to disclose sensitive information (e.g., substance abuse, sexual orientation). In this study, participants listened to a taped depiction of a medical visit in which a physician gave an assurance of either absolute or relative confidentiality, or made no mention of confidentiality whatsoever. Those who listened to the physician give an assurance of confidentiality (either relative or absolute) indicated a greater willingness to disclose information to the physician than those in the condition where confidentiality was not raised (see also Nowell & Spruill, 1993). Despite its demonstrable benefits to client outcomes, the actual operation of confidentiality has proven to be particularly troublesome.

Central to these troubles are the increasing demands placed on professionals to disclose confidential information to third parties such as employers, police, credit agencies, and insurance companies (Bok, 1984; Bollas & Sundelson, 1995; Gellman,

1986; Lindenthal et al., 1984; Lindenthal & Thomas, 1980). The anxiety generated by these pressures is compounded by the many lawsuits that have been successfully waged against professionals for inappropriate non-disclosure of confidential information. The most famous is arguably *Tarasoff vs. The Regents University of California* where in 1969, a young university student, Tatiana Tarasoff, was murdered by an obsessed and schizophrenic admirer, Prosenjit Proddar, two months after he informed his therapist of his intention to do so (see Simone & Fulero, 2001). While the therapist advised the police of Proddar's intention, Tarasoff herself was not warned, a decision made in the interests of confidentiality. The court found the therapist liable for failing to warn Tarasoff and sanctioned severe penalties for non-disclosure of confidential information when one's clients are likely to pose a risk to others. The *Tarasoff* case is widely regarded by psychological clinicians as the beginning of the erosion of confidentiality (Bok, 1984; Vandecreek & Knapp, 2001).

Clearly, the management of client-confidentiality involves the recognition and resolution of 'disclosure dilemmas'. On one side of the dilemma, confidentiality exists as a highly-valued principle of professional practice, securing positive outcomes for the client and pressuring professionals to keep client information concealed. Any decision to disclose is likely to be seen by the client as a betrayal of trust, which may have been difficult to obtain and virtually impossible to restore (Hook & Cleveland, 1999). On the other side, the professional faces increasing pressures to disclose confidential information and any decision to not to do may risk *Tarasoff*-type consequences. On both sides, the professional faces sanctions if they can be shown through legal or ethical processes to have 'got it wrong'. The complexities of confidentiality as a process can be depicted using the conceptual framework outlined earlier, as shown in Figure 3.4.

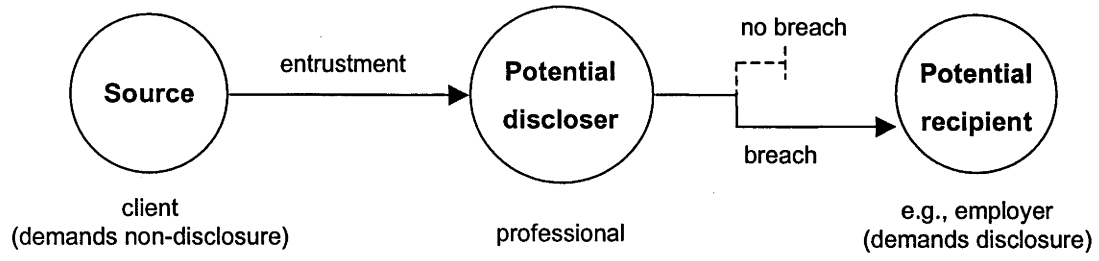


Figure 3.4 Confidentiality as a three-party disclosure dilemma.

Rather than examining how professionals resolve these dilemmas, the bulk of the psychological literature on confidentiality seeks to identify their causes. Two broad themes have emerged from this work. This first is that formal rules prescribing appropriate disclosure of confidential information lack the specificity needed to avoid these dilemmas (Hook & Cleveland, 1999; Jacques & Folen, 1998). For instance, regulations stating that one must disclose when harm is likely to befall others generally leave it to the clinician to define "harm" and "likely" for themselves (Hook & Cleveland, 1999; see also Knowles & McMahon, 1995). The second theme is that these formal rules are *incompatible* with real-world demands associated with the practice of so called "confidence work" (Barbour, 1994, p. 148). This is particularly true in clinical settings where the increasing number of interdependent professionals involved mean that disclosure boundaries are constantly revised and re-negotiated, as suggested by Barbour (1994) below:

> Even where restrictions, regulations or guidelines exist, they cannot hope to cover all eventualities or permutations involved in the complex web of relationships and circumstances surrounding work with HIV seropositive individuals...Similarly, such guidelines cannot cover all staff working or associated with the complex organizations in which 'confidentiality' is located, which ensures that its realisation, if ever possible, is problematic (p. 147).

Against this backdrop, a small number of researchers have examined the process whereby confidentiality dilemmas are resolved. In one study, Lindenthal and Thomas (1980) presented clinicians (in this case, medical internists, psychologists and psychiatrists) with a series of vignettes depicting a client involved in various activities that posed a risk to social order. Relatively 'low-risk' vignettes depicted the client

involved in activities like shoplifting and reckless driving, whereas relatively 'high-risk' vignettes depicted pyromania, rape, and murder. Clinicians were required to respond to each vignette by stating what they would do if this was a client in their care. Specifically, whether they would (a) disclose knowledge of the client's involvement to others (i.e., breach confidentiality) or (b) not disclose this knowledge (i.e., maintain confidentiality). Results indicated that as the risk posed to social order grew progressively more severe, clinicians' willingness to breach confidentiality increased. Specifically, when non-disclosure had low-risk consequences clinicians preferred maintaining confidentiality, whereas when it had high-risk consequences they preferred its breach. When the risk associated with non-disclosure of the confidential information was moderate, clinicians were left largely undecided as to what to do. In follow-up research, Lindenthal et al., (1984) included vignettes in which the client posed a risk to themselves (e.g., suicidal ideations). Again, clinicians were presented with the vignettes and asked to indicate the course of action they would follow. As before, clinicians were most willing to disclose when non-disclosure posed a major risk to social order (e.g., a client who threatened to plant a bomb) but were less willing to disclose when the client posed a risk to themselves, that is, when they reported suicidal ideations or behaviour. Lindenthal et al., (1984) argued that non-disclosure was preferred under these circumstances because disclosing would betray the client's trust, do little to prevent their actual suicide, and deter the client from seeking help in the future (see also Lindenthal, Jordan, Lentz, & Thomas, 1988).

More recently, Knowles and McMahon (1995) examined public perceptions about psychologists' obligations to disclose confidential information. Participants in this study were presented with statements describing situations where a psychologist might disclose confidential information (e.g., to save a life, to prevent a murder). Following this, they were asked to respond to each statement by indicating what they thought a psychologist *would* and *should* do in that particular situation. Results indicated a close concordance between these two issues, and reflected the pattern found by Lindenthal and his colleagues. Specifically, participants believed that non-disclosure is paramount when the client poses a minor risk to others (e.g., illegal drug use, theft) but that disclosure is paramount when the client poses a major risk to others

(e.g., murder). Interestingly, the only situation that participants remained undecided about related to a client taking part in treason or the sabotage of national interests.

This 'situational fluidity' with which confidentiality dilemmas are resolved is neatly captured in an ethnographic study of AIDS care workers by Barbour (1994). These workers reported continual pressures to disclose information about the HIV status of their clients by social workers, paediatricians, and midwives, which were always refused on the grounds of preserving confidentiality. Yet, workers often tried to disclose this information to people they knew to be close to the client (e.g., past sexual partners) without committing an explicit breach of confidentiality. In these situations, the risks associated with non-disclosure, particularly secondary HIV infection, dominated workers' thinking.

Summary and implications

From the work outlined above, it is clear that risk is a central theme in the psychological literature concerning the management of confidentiality, as it is in the self-disclosure literature. With respect to self-disclosure, risk relates primarily to the possible consequences of a decision to disclose, for example, being rejected or betrayed. However, in the confidentiality literature, risk relates primarily to the possible consequences of *not* disclosing, that is, of maintaining confidentiality. The argument here is that as the risk associated with non-disclosure grows progressively more severe, the likelihood of breaching the formal conditions of confidentiality (i.e., disclosing) also increase. As a result, the confidentiality literature provides a neatly encapsulated study of *when* people might breach formal rules in order to avoid problematic non-disclosure (e.g., *Tarasoff*-type situations). Obviously, it would be of great value to know *if* and *when* ADF personnel are likely to 'override' official rules governing disclosure of classified information in order to avoid problematic non-disclosure. As alluded to above, knowing when people might takes steps to avoid problematic non-disclosure can also reveal when they might not.

For now, a parallel can be drawn between the practice of confidentiality and the 'appropriate' disclosure of classified information in defence organizations. For both, formal rules prescribing what is appropriate exist and are reinforced by the

prospect of punishment for their breach. As discussed above, those pertaining to confidential information are widely believed to lack the specificity needed to avoid disclosure dilemmas and to be incompatible with 'real-world' demands. As yet, no commensurate argument has been forthcoming *vis-à-vis* the rules pertaining to classified information however the context surrounding the disclosure of classified information is similar in many ways to that which nurtures confidentiality dilemmas. Like 'confidence work', military activities (particularly operations) take place in a context characterised by high degrees of uncertainty and unpredictability. Indeed, the breakdown of the 'certainty' associated with the bi-polarity of the Cold War has meant that the activities which military forces must now perform (e.g., peace-keeping, stabilising failed states) are more diffuse and less predictable in nature than ever before (Dorman et al., 1998). Furthermore, and as with confidence work, the solution of these problems demands that military personnel must work in a more *interdependent* fashion than before, increasing the potential for one's decisions to affect, and be affected by, the decisions of others. As is outlined in the confidentiality literature, such factors can limit the extent to which actual disclosure outcomes mirror a formal blueprint.

While the confidentiality literature reviewed above provides some insight into how risk may motivate people to breach official rules so as to avoid problematic non-disclosure, it offers little detail about *who* one will breach for in this respect. This idea has been investigated, however, in the context of a third disclosure phenomenon known as 'whistle-blowing'.

'Blowing the whistle': Prosocial disclosure

Whistle-blowing is "the disclosure by organization members (former or current) of illegal, immoral or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action" (Near & Miceli, 1985, p. 4). As with confidentiality, two types of whistle-blowing are distinguished: internal and external (Near & Miceli, 1985, 1996). *Internal* whistle-blowing, the more common type (Rothschild & Miethe, 1999), refers to circumstances where the disclosure is made to other members of the organization. For example, the catastrophic loss of the space shuttle *Challenger* occurred months after a NASA

engineer disclosed information about the potential problems with the "O-Rings" on the vehicle's booster rockets to management (see Greenberger, Miceli, & Cohen, 1987; Miceli & Near, 1988). The failure of internal whistle-blowing to invoke corrective action is frequently cited as the main cause of the second type, *external* whistle-blowing (Near & Miceli, 1996; Rothschild & Miethe, 1999), that is, where the disclosure is made to parties outside the organization, such as the media or regulatory bodies. Clearly, the consequences of having an organization's wrongdoings exposed to an external audience are likely to be worse than those of disclosures that are kept 'in-house' (Greenberger et al., 1987; Near & Miceli, 1996). For instance, external whistle-blowing often decreases public trust in the organization and undermines the organization's authority structure (Greenberger et al., 1987). Further, despite the fact that both internal and external whistle-blowers often experience organizational retaliation (Near & Miceli, 1986, 1996; Rothschild & Miethe, 1999), external whistle-blowers are generally subject to more severe retaliation (see Greenberger et al., 1987). For example, when Kermit Vandivier, an engineer at the BF Goodrich company, told the FBI that his employer had falsified test results concerning the safety of its aircraft brakes, he was repeatedly threatened by the organization and told to 'keep quiet' (see Vandivier, 1972).

It is clear, particularly when threats of organizational retaliation are involved, that whistle-blowing is not primarily confined to the whistle-blower and the recipient as some have implied (e.g., Gundlach, Douglas & Martinko, 2003). Instead, whistle-blowing must be conceived of as a phenomenon that also involves other parties capable of influencing the potential discloser in their decision making, including members of one's work group and the organization's management. For example, co-workers may fear that disclosure of illegal management activities would put their jobs at risk, and they may therefore discourage whistle-blowing through group norms (Greenberger et al., 1987). Of course, the extent to which these parties act as true 'sources' of the relevant information varies (Gundlach et al., 2003). In some cases, these parties entrust the potential whistle-blower with the information directly, while in others, the whistle-blower may simply happen across the information unbeknownst to others. Either way, third parties such as management and co-workers are able to exert considerable influence over the potential whistle-blower's decision and therefore

must be included in any conceptualisation of the phenomenon, as depicted in Figure 3.5.

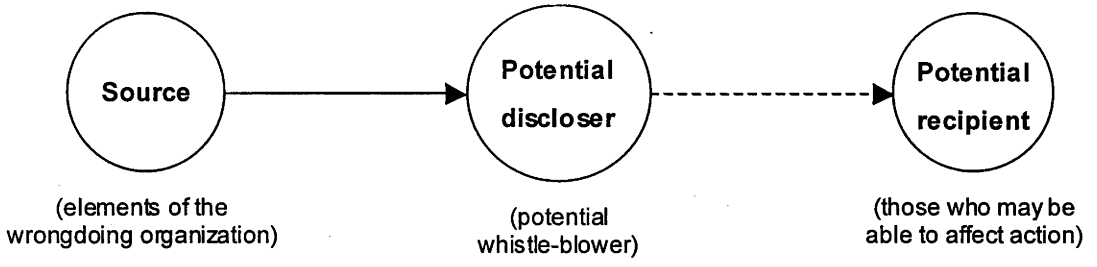


Figure 3.5 Whistle-blowing as a three-party process.

Efforts to determine the psychological factors affecting a decision to 'blow the whistle' have turned up, to some extent, ideas evident in the confidentiality literature. Specifically, the potential whistle-blower is conceived of as someone who 'weighs up' the risks associated with disclosure (e.g., management retaliation, loss of job) and non-disclosure (e.g., possible harm befalling others; see Dozier & Miceli, 1985; Greenberger et al., 1987; Gundlach et. al., 2003). However, unlike the work relating to confidentiality, researchers of whistle-blowing have framed this process within a broader social context which, they argue, helps explain why whistle-blowing occurs despite the risk of severe retaliation. Specifically, whistle-blowing is conceived of as a type of *prosocial behaviour* (Brief & Motowildo, 1986; Dozier, & Miceli, 1985; Gundlach et al., 2003; Miceli, Dozier, & Near, 1991; Miceli & Near, 1988; Street, 1995).

Prosocial behaviour is behaviour intended to benefit others such as helping, sharing, donating and volunteering (Brief & Motowildo, 1986). Hence, prosocial behaviour is similar to altruism, yet whereas altruism is behaviour in which the actor does not expect to receive material or social rewards themselves, the concept of prosocial behaviour allows for some degree of self-interest on the part of actor (Dozier & Miceli, 1985). With this in mind, research interest in the psychological factors affecting people's willingness to blow the whistle has focused largely on individual difference factors that would appear to be logical predictors of prosocial

behaviour. In other words, the psychology of whistle-blowing represents, by and large, the search for the archetypal 'whistle-blower' personality.

In this vein, Brabeck (1984) argued that willingness to blow the whistle will likely be related to level of 'moral reasoning'. To investigate this, Brabeck measured people's level of moral reasoning, classifying them as either 'conventional' in this respect (i.e., only concerned with seeking approval and respecting authority) or 'principled' (i.e., concerned with safeguarding the rights of all). Participants in this study were then exposed to a serious error in an article they were led to believe was about to be published by an authority figure, in this case, a professor. A decision to inform the investigators of the error was taken as a measure of one's willingness to blow the whistle. As hypothesized, results indicated that those with the higher 'principled' level of moral reasoning were more willing to disclose the error than their conventional counterparts. While this scenario represents what can only be described as a 'mild' version of whistle-blowing (the whistle-blower faced no prospect of retaliation by the professor) similar results are reported by Jos, Tompkins, and Hays (1989) who examined the personalities of actual whistle-blowers. In this research, whistle-blowers were found to be more committed to ideas of universal morality and social responsibility and less committed to relativistic claims about moral rules, than non-whistle-blowers. Yet, inferring causality is clearly problematic. It is possible, for instance, that whistle-blowers began to portray themselves in this light only after they engaged in such whistle-blowing activity.

Other research has failed to associate personality factors with whistle-blowing. Rothschild and Miethe (1999) for instance, took a number of individual difference measures from both internal and external whistle-blowers, as well as 'non-observers' (i.e., those who had not observed misconduct) and 'silent' observers (i.e., those who had observed misconduct but decided against disclosing it). Results showed no difference between the groups on measures of social responsibility and beliefs about altruism and only a slight but non-significant trend for whistle-blowers to score higher than non-whistle-blowers in terms of commitment to universalistic values. Rothschild and Miethe (1999) concluded that whistle-blowing is better understood as a dynamic form of worker resistance than an outcome of dispositional characteristics.

Miceli et al., (1991) also casts doubt on the idea of a model whistle-blower personality. In this study, participants completed a scale measuring their level of moral development and were then asked (at a much later point in time) to take part in a job applicant selection task. The task involved rank-ordering three hypothetical job applicants, one of which was clearly the most superior applicant. While performing this task, participants were informed that, in the past, the study had failed to yield good results and to be publishable, participants should 'fudge' their rankings by rating a less suitable applicant as the preferred candidate. Participants were then left alone to complete the task before a confederate of the experimenters entered (under the guise of an 'ethics inspector') and asked participants to write down anything they had been asked to do during the study which they considered to be objectionable. A decision to blow the whistle was taken as a 'yes' response to this question and a subsequent description of the "fudging" request. Curiously, results indicated that as the participant's level of moral development increased, willingness to blow the whistle *decreased.*

Summary and implications

As outlined above, whistle-blowing is widely considered to be a form of prosocial behaviour. That is, it is viewed as behaviour that is intended to benefit others, whether they be other members of the wrongdoing organization, particular social groups, or the broader society. Despite the fact that this prosocial perspective has translated, by and large, into an inconclusive search for the typical whistle-blower personality, the idea of disclosure as prosocial behaviour is relevant to the disclosure of classified information in the ADF, albeit in two different ways.

First, the disclosure of classified information in military organizations like the ADF may, at times, actually constitute whistle-blowing. Despite being a 'legitimate' form of information control, the classification system employed by defence organizations has concealed activities which are immoral, illegitimate, or illegal, such as U.S. military research concerning the effects of radiation exposure on military personnel (Aftergood, 2000). Further, history has shown that defence personnel will disclose such information on occasions, despite formal and informal pressures not to do so, for example, when Daniel Ellsberg disclosed the 'Pentagon Papers' to the New

York Times in 1971 (see Ellsberg, 2003). The aim of this thesis, however, is to understand the psychological factors affecting the disclosure of classified information as it *routinely* occurs, not when it manifests as whistle-blowing. To this end, the idea of disclosure as prosocial behaviour is relevant in a second way.

With its 'prosocial' focus, the whistle-blowing literature makes salient the idea that disclosure and non-disclosure outcomes can reflect interpersonal or intergroup cooperation. While the emergence and sustainment of cooperation is paramount to the effectiveness of defence organizations like the ADF, appropriate disclosure and non-disclosure of classified information is a critical, if not *the most critical* form of cooperation in the modern military organizations. A lack of cooperation in this respect effectively denies the organization the ability to achieve its goals, and opens the way for disaster, as has been discussed in the first two chapters. Conceiving of disclosure outcomes in the ADF as reflecting cooperation (or non-cooperation) opens the way for new light to be shed on the research issue. Yet, the whistle-blowing literature fails to provide an adequate account of the psychology of disclosure as a cooperative activity because researchers in the area have remained fixated on factors 'within' the whistle-blower, that is, personality factors. The cost has been a neglect of factors relating to the whistle-blower's relationship with both the organization and the potential recipient of the information. While some relational terms including 'loyalty' and 'commitment' have received brief mention (e.g., Near & Miceli, 1996; Street, 1995), we must look further afield to find a deeper appreciation of how the potential discloser's relationship with the source and potential recipient is likely to impact on their decision-making. To this end, we next consider the literature devoted to the concept of *secrecy*, within which the potential discloser's affiliations and group memberships come to the fore.

Secrecy: The role of group affiliation

A century ago, Georg Simmel laid the foundations of social-scientific interest in secrecy. All interpersonal and intergroup relationships, Simmel (1906) argued, are characterized by a "ratio of secrecy" (p. 462), without which certain ends cannot be achieved (see also Simmel, 1950). Since Simmel's writings, secrecy has attracted scholarly attention from within psychology (Fine & Holyfield, 1996; Shlien, 1984)

sociology (Bellman, 1981; Shils, 1956) and anthropology (Merten, 1999; Tefft, 1980) and has thus been discussed with respect to individuals, groups, organizations, and entire societies. Despite the multidisciplinary interest, all definitions of secrecy share the same core, that is, the intentional or 'calculated' concealment of information (Bok, 1984; Erickson, 1979; Kelly, 2002; Redlinger & Johnson, 1980; Tefft, 1980; Wilsnack, 1980). Of course, there are variations on this theme, particularly when the aim has been to distinguish secrecy from privacy. For example, Warren and Laslett (1977) separate the two according to *content*, viewing secrecy as a strategy for concealing illegal/deviant activities and privacy for concealing moral/legitimate activities. Alternatively, Shils (1956) focuses on the *consequences* of disclosing that which is concealed, defining secrecy as compulsory concealment "reinforced by the prospect of sanctions for disclosure" (p. 26) and privacy as voluntary concealment where the discloser remains immune from sanctions (see also Kelly & Carter, 2001).

By focusing on the content of what is being concealed or the consequences of its disclosure, these definitions downplay the existence of secrecy as a general social process. Clearly, secrecy conceals moral and legitimate activities as well immoral and deviant ones. Further, disclosing is an inherent part of the practice of secrecy not its logical opposite, or as Bellman (1981) suggests "[t]o tell a secret is to *do* secrecy. The methods used in that accomplishment are in part constitutive of the phenomenon" (p. 8). Bellman (1981) offers a 'neutral' view of secrecy designed to capture the phenomenon more generally, defining secrecy as the process by which concealed information is managed or controlled.

Clearly, secrecy overlaps with the other phenomena discussed above. Self-disclosure, confidentiality, and whistle-blowing all involve intentional concealment and disclosure of information. Indeed, discussions of these phenomena draw heavily on the terms "secrecy" and "secret". Self-disclosure is seen as the revelation of one's 'personal secrets' (Kelly & Carter, 2001; Vrij et al., 2002), confidentiality is often termed 'professional secrecy' (Bok, 1984), and whistle-blowing involves the airing of an organization's 'dirty secrets' (see Messick, 1999). However, other secrecy phenomena have also captured the interest of those working from a psychological framework including organizational and family secrecy, and so-called 'secret-societies', that is, groups in which participants are linked via secret activities (B. H.

Erickson, 1981). Many factors thought to affect disclosure outcomes *vis-à-vis* these phenomena have been discussed in the preceding pages. Analyses of organizational secrecy and of secret societies, for instance, draw attention to how the trustworthiness of the potential recipient impacts on people's willingness to disclose (Erickson, 1979; B. H. Erickson, 1981; Ponse, 1976). Additionally, notions of disclosure reciprocity and prosocial behaviour are implicated in analyses of organizational secrecy. For example, in their study of a voluntary mushroom-collecting society, Fine and Holyfield (1996) found that members often disclosed information about their secret picking spots on the expectation that the recipient would reciprocate at some later point in time. Similarly, Galnoor (1975) claims that obligations of reciprocity constitute "the unwritten rules" (p. 40) of government secrecy, but provides little data in support of this claims. Despite the overlap, discussions of family and organizational secrecy and of secret societies draw attention to another factor that receives only scant attention in the literatures discussed earlier - the potential discloser's affiliations and group memberships.

Vangelisti and Caughlin (1997) examined how a sense of affiliation with both family members and the potential recipient influenced people's willingness to disclose family secrets. In this study, participants were instructed to recall and describe a family secret and to rate the likelihood of disclosing it to: (a) their girl/boyfriend, (b) their best friend, (c) a friend, (d) a co-worker/classmate, or (e) an acquaintance. They were then asked to rate their level of satisfaction with their family relationships and the extent to which they were 'psychologically close' to the potential recipient. Results indicated that those who were unlikely to disclose the family secret had stronger family relations than those who were moderately or highly likely to disclose the secret. Further, those highly likely to disclose rated themselves as psychologically closer to the potential recipient than those unlikely to disclose. The idea that a sense of affiliation underpins non-disclosure is also evident in accounts of secret societies (see MacKenzie, 1967 for a review). B. H. Erickson (1981) for example, analysed the structure of six secret societies including the Auschwitz and Norwegian underground, the Chinese White Lotus sect, the Lupollo crime family, and the San Antonio and Cheltenham illegal drug markets. Results showed that non-disclosure of information *within* these societies reflected intergroup divisions that existed prior to the society's inception. These "relational cleavages" (B. H. Erickson, 1981, p. 196) manifest as

separate branches of the society, representing members' perceptions about who were the most trustworthy members.

While these studies focus on affiliation and disclosure outcomes in families and secret-societies, other research has examined the impact of affiliation and group membership on organizational disclosure outcomes. For example, in a study of how police officers regulate their disclosures to news reporters, Ericson (1989) found that officers categorized reporters into one of two groups: *inner-circle* or *outer-circle.* Inner-circle reporters were those sympathetic to the police and willing to publish only 'positive' stories, and were therefore considered 'part of the team'. Outer-circle reporters in contrast, were not sympathetic to the police and were most interested in exposing police impropriety and mismanagement, thereby constituting a clear 'out-group'. Not surprisingly, Ericson (1989) found that secret information flowed along the contours of this categorization - toward inner-circle and away from outer-circle reporters. In this vein, Wetzel and Wright-Buckley (1988) sought to determine whether disclosure reciprocity could be achieved in the context of a bi-racial therapy setting. In this study, a sample of African-American women were placed in a situation where they could talk to, but not see, the therapist. Half were shown a photograph depicting the therapist as a white female while the other half were shown a photograph depicting the therapist as a black female. Results indicated that participants were more willing to reciprocate disclosures when they believed she was a fellow African-American than when they believed she was white (see also Poston, Craine, & Atkinson, 1991; Rotenberg, 1986). While not organizational in nature, Hargie et al., (2002) report a similar theme in a study of self-disclosure amongst Catholic and Protestant youths. Here, participants rated their willingness to disclose various items of personal information to: (a) strangers of the same religion, (b) strangers of the other religion, (c) a friend of the same religion, and (d) a friend of the other religion. Results showed that while friends were more likely to be disclosed to than strangers, co-religionists were preferred as potential recipients over 'other-religionists'.

According to Yovetich and Drigotas (1999) the idea of affiliation as it applies to disclosure outcomes is better thought of as 'relative intimacy'. They asked people to list ten others with whom they were personally acquainted (e.g., casual friends,

romantic partners, relatives, and so on) and to rate the level of intimacy they shared with each. They were then asked to imagine that the person at the top of the list had disclosed secret information to them, and to rate their likelihood of disclosing this information to each of the other people on the list. This process was repeated for the second person listed, and so on, until each of the acquaintances had taken on the role of the source. Results showed that participants were more likely to disclose 'upward' (i.e., from a lower- to a higher-level intimate) than 'downward' (i.e., from a higher- to a lower-level intimate) leading Yovetich and Drigotas (1999) to conclude that "[i]t is not simply a matter of being close to the target but of being closer" (p. 1146).

However, a large and influential body of work in social psychology has conceived of the mechanism underlying people's group affiliations in terms of 'social identification' processes (Tajfel & Turner, 1979; Turner, 1991; Turner et al., 1987). One of the core ideas here is that people derive a 'social identity' from the groups and categories to which they belong (Tajfel & Turner, 1979). Specifically, a social identity is understood as a *self-definition* in social rather than personal terms, for example, 'we pilots' or 'we soldiers' (Onorato & Turner, 2002, 2001; Turner et al., 1987). Over the past three decades, a large body of work has shown that people seek to promote the interests of those groups and categories from which they draw a valued social identity or 'sense of self' (e.g., Ellemers, 2001; Ellemers, de Gilder, & van den Heuvel, 1998; van Knippenberg & Sleebos, 1999). Moreover, research has shown consistently that people tend to perceive others with whom they share a sense of social identity ('ingroup members') more positively than those with whom they do not ('outgroup members). For instance, ingroup members are generally perceived as more trustworthy and likeable than outgroup members (Brewer, 1981; Kramer, 2001). With this broader theoretical tradition in mind, the argument put forward by Yovetich and Drigotas (1999) can be redefined in terms of social identification processes. That is, the 'relative intimacy' with which one perceives the potential recipient of one's secrets reflects the extent to which they share a salient social identity, that is, the extent to which they are perceived as either an ingroup or an outgroup members.

Indeed, work to this end has been recently conducted by Dovidio et al., (1997). These authors argued that self-disclosure (amongst other things) is likely to follow the contours laid down by one's social identities. As a result, they hypothesized that

people should be willing to disclose secret information about themselves to those previously categorized as outgroup members in situations where these individuals can be 'recategorized' as ingroup members. To test this idea, Dovidio et al., (1997) had people work together as members of two three-person groups (A and B). They then manipulated participants' view of the situation in a way that enhanced either a sense of inclusiveness or divisiveness. In the inclusiveness condition, participants were seated at a hexagonal table in an interspersed manner (i.e., ABABAB), were given a new 'one group' name and received other instructions that emphasized a sense of common identity. In the divisiveness condition, participants sat on opposite sides of the table (i.e., AAABBB) and no mention was made of any common identity. Subsequently, the experimenters placed participants into dyads composed of either two original group members (i.e., AA, BB) or two separate group members (i.e., AB, BA), and provided them with a list of discussion topics, asking which topics they would be most willing to discuss with their dyad partner. Upon ostensibly choosing a moderately intimate topic ("What are you most afraid of?") participants took part in a five-minute taped discussion with each other, after which the experimenters coded the discussion for the amount or depth of intimate information disclosed. Results supported the hypothesis in that the inclusive one-group representation reduced the extent to which participants favoured members of their original group in terms of their self-disclosures. Dovidio et al., (1997) thus concluded that by changing who people perceive as 'ingroup members' (those sharing a social identity), one can change the overall pattern of self-disclosure.

Summary and implications

Secrecy, the process by which restricted or concealed information is controlled (Bellman, 1981), encompasses those phenomena which have been discussed so far and a number of others, notably family and organizational secrecy and secret societies. To some degree, the factors thought to underpin disclosure outcomes in these contexts mirror those discussed earlier. For example, trust is a salient consideration for the potential discloser in each of these phenomena, either with respect to the source, the potential recipient, or both. Yet, the secrecy literatures discussed above draw attention to a broader factor thought to affect disclosure outcomes. This factor is the potential discloser's affiliations and group memberships

and can be represented as shown in Figure 3.6. Indeed, this factor may be capable of providing a more sophisticated understanding of *when* and *why* the potential discloser will uphold the trust of the source or when and why they will place trust in a given recipient (Yamagishi, Foddy, Makimura, Matuda, & Platow, 2003; see also Brewer, 1981; Williams, 2002).

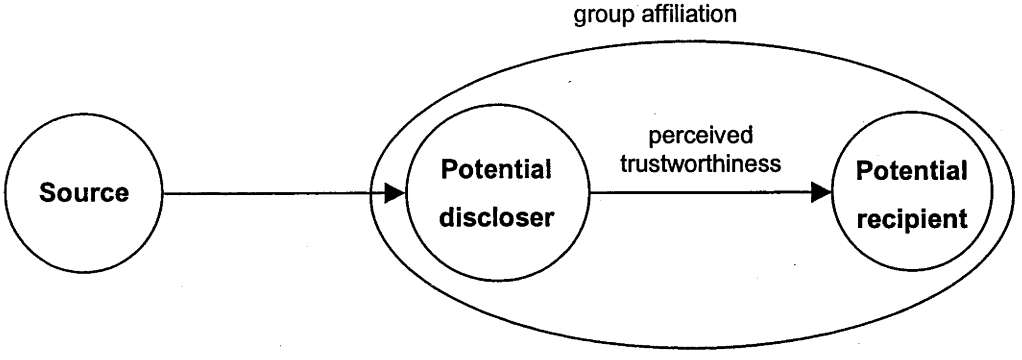


Figure 3.6 Secrecy as moderated by group affiliation.

For now however, we can propose a general hypothesis that disclosure outcomes will follow the contours of those affiliations and group memberships that are psychologically significant to the potential discloser, and that this 'psychological significance' will likely involve a sense of shared social identity. Our question now concerns the extent to which these ideas are likely to be relevant to disclosure outcomes in the ADF as they apply to classified information.

We can go some way toward arguing for their relevance by drawing attention to the strong sense of affiliation, allegiance and shared group membership that is a hallmark of military life, particularly with respect to one's chosen Service. The three Services of the ADF possess strong and distinctive cultures and histories, reinforced by training and Service enculturation programs. One could conclude therefore, that any general hypothesis about disclosure outcomes *vis-à-vis* classified information following the contours affiliation and shared group membership must be made with regard to personnel's Service.

General summary and conclusions

Psychology has made considerable progress toward understanding the factors affecting human disclosure behaviour as it relates to particular social phenomena. For the moment, these phenomena do not include the disclosure of classified information in contemporary military/defence organizations. However they do include broadly comparable phenomena such as confidentiality and, more generally, secrecy. They also include other phenomena in which the potential discloser of information is central, notably self-disclosure and whistle-blowing. If we are to accept human disclosure behaviour as a *field* of psychological enquiry then (see Wagner & Berger, 1985), it is one that is heterogenous to the core and primarily 'phenomenon-driven' rather than 'theory-driven'. This chapter has reviewed these contributions and assessed their relevance insofar as helping us gain an understanding of the psychology that underpins the disclosure and non-disclosure of classified information in contemporary defence contexts.

On the basis of this review, it is possible to distil two broad factors that are likely to be implicated in the disclosure of classified information in some way. The first of these is *risk*, that is, the prospect of loss (Smithson, 1994). The idea that disclosure outcomes can be shaped by the potential discloser's perceptions of risk is present in both discussions of self-disclosure and about the practice of confidentiality. The dominant theme in the self-disclosure literature is that disclosure of personal information is risky and thus necessitates the placement of trust in the potential recipient. The dominant theme in the confidentiality literature however is that *non-disclosure* of confidential information is risky by virtue of possible 'Tarasoff-type' consequences, and that these risks place a strain on the trust between the potential discloser and the source (i.e., the client). While both themes offer useful starting points for an analysis of the psychology underpinning problematic non-disclosure of classified information, it is the work conducted with regard to confidentiality that is particularly helpful here. This work explicitly examines when perceived risks will and will not lead people (in this case, professionals) to 'override' official rules mandating the non-disclosure of information, hence it addresses the issue of problematic non-disclosure directly. In so doing, it provides both a conceptual and methodological 'template' for an initial exploratory investigation of when perceived

risks will and will not lead ADF personnel to override the formal rules mandating the non-disclosure of classified information.

The second factor that can be distilled from the review above is the notion of affiliation or, more generally, shared group membership. The idea that disclosure outcomes follow the contours of one's group affiliations is particularly salient in the literature examining the practice of secrecy in families, organizations, and secret societies. Being phenomenon- rather than theory-driven however, little insight has been forthcoming as to *how*, psychologically speaking, disclosure outcomes are mediated by an individual's affiliations and shared group memberships. We have suggested that the concept of identification may be particularly useful in this respect. Again, this work provides a useful starting point from which to investigate disclosure outcomes with respect to classified information in the ADF. Specifically, we can add this factor to the plan outlined above, so as to examine not only *when* perceived risks will and will not lead ADF personnel to override the formal rules mandating non-disclosure, but *for whom* such disclosures will be made and for whom they will not.

An argument could be made for the presence of a third general factor from the review above, that is, trust. Clearly, trust is a significant determinant of disclosure outcomes across each of the phenomena discussed above, and is relevant to the potential discloser's relationship with both the source and the potential recipient. In that respect, trust emerges as a kind of 'master variable' of human disclosure behaviour. Having said that, trust is also understood within these literatures as an *outcome* variable, that is, a *product* of affiliation and that which is necessitated by the presence of risk. In this light, trust exists as more of a 'second-order' factor than a master variable. This by no means should imply that the role of trust will not be attended to within the context of this thesis. However in terms of setting up a broad conceptual framework, the emphasis is better placed on the fundamental factors of risk and affiliation. Our empirical investigation into the role of these factors in shaping disclosure outcomes in the ADF context begins in the next chapter.

CHAPTER 4

THE ISSUE OF BREACH BEHAVIOUR:

IF, WHEN, AND FOR WHOM?

Introduction

As was argued in the previous chapters, an adequate understanding of problematic non-disclosure as it might apply to classified information in a modern military setting requires we approach the problem from a psychological perspective. So far, psychology has made considerable progress toward understanding the factors underpinning other disclosure phenomena and this progress was reviewed in Chapter 3. Self-disclosure, breaches of confidentiality, whistle-blowing, and various forms of secrecy have received the most attention in this respect. At one level, these phenomena appear relatively distinct from one another. Yet, at another they share a common core in that each involves an individual faced with a decision to either disclose or withhold concealed information. That is, an individual takes the position of the 'potential discloser'. From the review, two broad factors emerged as potentially relevant to an analysis of problematic non-disclosure *vis-à-vis* classified information. The first is risk as it relates to the consequences of both disclosing and not disclosing. The second is the potential discloser's affiliations or, more generally, their group memberships.

The aim of this chapter is to investigate in an initial study how these factors influence the disclosure and non-disclosure of classified information amongst ADF personnel. As alluded to earlier, a good starting point in this respect would be to determine if and when the consequences associated with non-disclosure will (and will not) lead ADF personnel to breach the official rules regarding access to classified information. Put another way, when will personnel commit a breach of national security to avoid problematic non-disclosure and when will they not? Clearly, this mirrors the work examining how professionals 'weigh-up' the risks before deciding whether to breach client-confidentiality (Lindenthal et al., 1984; Lindenthal & Thomas, 1980). However, we seek to extend this idea by investigating not only *when*

ADF personnel will and will not override official rules to avert problematic non-disclosure but *for whom* they will do so. In other words, will the potential discloser's affiliations, particularly with their chosen Service, make any difference in this regard?

By examining if, when and for whom ADF personnel will breach national security to avoid problematic non-disclosure, the notions of 'organizational betrayal' and 'leaks' of classified information become relevant. The chapter begins with a brief review of the literature relating to these concepts before moving on to the empirical work. Two studies are presented in this chapter. The first is a pilot study involving a sample of civilian defence scientists governed by the same rules relating to the disclosure of classified information as their ADF counterparts. The second study (Study 1) is a refinement of the pilot that involves a larger sample of ADF personnel. Both employ a scenario-based methodology to manipulate the expected consequences of non-disclosure. In Study 1, these consequences are harm to either an ADF colleague, an ADF Service, or the ADF globally. In this order, we see these consequences as constituting a continuum of increasing risk that will dictate the extent to which ADF personnel will be prepared to breach national security. However, a number of 'variants' are made to this basic template, one of which is whether the non-disclosure will harm one's own Service or another Service.

Leaks and organizational betrayals

As implied above, a breach of national security involving the 'unauthorised' disclosure of classified information can be viewed as an organizational betrayal (Sarbin et al., 1994). Recently, Elangovan and Shapiro (1998; see also Jones & Burdette, 1994; Morris & Moberg, 1994) defined the notion of organizational betrayal as:

> [A] voluntary violation of mutually known pivotal expectations of the trustor by the trusted party (trustee) which has the potential to threaten the well-being of the trustor" (p. 548).

According to these authors, two types of organizational betrayal can be discerned. The first, *accidental betrayal*, refers to violations of trust that take place without the trustee intending to do so (e.g., a member of staff inadvertently emails employee

records to organizational members at large). The second and more frequent type, *opportunistic betrayal*, refers to violations of trust that occur with the intent of the trustee, but in response to particular situational demands (e.g., a captured soldier discloses the whereabouts of his unit colleagues to avoid torture). While most breaches of national security are accidental in nature (see Rumsfeld, 2002), we are concerned here with when and to whom ADF personnel will *intentionally* breach national security to avoid problematic non-disclosure. Hence, only the concept of opportunistic betrayal is relevant to the current discussion.

Of course, defence organizations like the ADF have long been interested in the factors leading personnel to intentionally betray national security via the unauthorised disclosure ('leaking') of classified information. This interest has tended to focus on personal characteristics of the potential discloser thought to be logical predictors of such behaviour. According to the conventional military wisdom, defence personnel engage in the unauthorised disclosure of classified information for one of four reasons, either: (i) money, (ii) ideology, (iii) compromise (e.g., blackmail), or (iv) ego-enhancement (Levchenko, 1988; Taylor & Snow, 1997)[4]. Clearly then, the military conceives of such disclosures as instances of organizational deviance, as illustrated by the current U.S. Secretary of Defense below:

> I have spoken publicly and privately, countless times, about the dangers of leaking classified information. It is wrong. It is against the law. It costs the lives of Americans. It diminishes our country's chance for success. (Rumsfeld, 2002, p. 1).

However, in conceiving of opportunistic betrayal more generally, Elangovan and Shapiro (1998) argue that a number of factors act as 'situational moderators' of the attractiveness of a decision to betray an organizational trust. Two factors are considered particularly important in this respect. First, whether or not an individual can expect to experience *severe punishment* for the betrayal and second, whether or not the individual can expect to be *identified* as the betrayer. According to Elangovan and Shapiro (1998), the 'right opportunity' for opportunistic betrayal is when the probabilities of being severely punished and of being identified are low.

---

3. The acronym 'MICE' is often used to summarise these factors (see Levchenko, 1988)

It is plausible that these factors may also influence the extent to which ADF personnel will be prepared to breach national security in the face of problematic non-disclosure. Yet in such situations, the identifiability of the potential discloser as a "betrayer" is likely to 'cut both ways'. In other words, one could be identified as a betrayer if they decide to disclose (i.e., by virtue of committing a breach of national security) and if they decide to not disclose (i.e., by those harmed by non-disclosure). In the former situation, one's expectations of being identified and of being punished are likely to be confounded to some degree. Put simply, one could expect to be identified as a betrayer in this respect through being punished for breaching national security since such punishments often manifest publicly (e.g., through loss of job or of one's security clearance). As such, it would be difficult to separate out the effects of expected identifiability and expected punishment in this situation. Yet, the prospect of being identified as a 'non-discloser' does not confound with expected punishment for no punishment is forthcoming in this situation (i.e., no breach of national security has been committed). Thus, expectations of being identified as a betrayer in this respect constitutes a form of risk independent of expected punishment.

In summary, an investigation of how risk (as it relates to consequences of non-disclosure) and group affiliation influence the disclosure of classified information brings forth a number questions: (1) Will prospective breaches of national security follow the continuum of the increasing risk (i.e., as non-disclosure harms a colleague, a Service, and the ADF, respectively); (2) Will it matter whether the Service harmed is one's own or not; and (3) Will the prospect of being punished or identified as a 'non-discloser' make any difference in this respect?

Clearly, there are sensitivities associated with asking military personnel if, when and for whom they are likely to commit a breach national security by disclosing classified information in a manner contrary to official rules. For one, this is an illegal behaviour that, as outlined above, is often considered to be an instance of deviance of the highest order. To some degree, this may be less so when the disclosure can be shown to have been brought about by problematic circumstances, as is the interest in this chapter. However, even in this context, participants are likely to be sensitive to whether they perceive their responses to be anonymous and the researcher to be

trustworthy and of legitimate intent. As a result, it would be necessary to obtain a number of official permissions to conduct the research from senior ADF officers including the respective Service Chiefs and the Vice-Chief of the Defence Force (VCDF). It would also be necessary to provide a number of verbal and written assurances to these individuals and to potential participants about the intent of the researcher.

To that end, it was considered appropriate for a pilot study to be conducted first so as to refine the research methodology and design before embarking on a major study involving ADF personnel. Therefore, the initial investigation involved a more convenient sample of personnel belonging to the Defence Science and Technology Organisation (DSTO), a research and development organization within Australia's Department of Defence. Importantly, DSTO personnel are bound by the same official rules and policies governing access to classified information as their ADF counterparts.

Pilot study

Sixty-seven defence scientists belonging to DSTO were asked to take part in the pilot study. Of these, the majority ($n = 47$) were men aged in their early thirties with most ($n = 56$) being employed at or above the middle-management level. Participants had been employed within the Department of Defence for an average of nine years[5].

Participants were informed that they would be taking part in pilot research that related to "information-sharing" in the work context. To this end, they were each asked to read three short scenarios that involved their hypothetical entrustment with 'work-relevant' information in some way. The first two scenarios detailed their entrustment with this information by a friend and by their workgroup, respectively. Here, participants were asked to simply imagine that the respective source had provided them with this information and trusted them not to disclose the information any further. In these scenarios no reference was made to the information being

4. Ethics approval for all studies reported in this thesis was obtained from the Australian National University Human Research Ethics Committee.

"classified". Instead, these scenarios served two specific purposes. The first was to provide an initial 'filler' task that would avoid participants being confronted from the very beginning with a scenario relating to their entrustment with, and prospective handling of, classified information. In other words, starting with two unclassified scenarios would likely 'ease' participants more comfortably into the research issue at hand. The second purpose was to broaden the empirical scope of the research somewhat, that is, to provide a means by which some insight could be gained into whether the factors affecting disclosure of classified information also affected the disclosure of work-relevant but *unclassified* information. As alluded to above, it was the third scenario that detailed participants' entrustment with classified information. Here, participants were asked to imagine that, as part of their normal DSTO duties, they had been unofficially requested to provide classified information to another part of DSTO.

Each scenario provided the backdrop to a number of 'disclosure dilemmas' that were formed using two factors. The first was the *consequence of disclosing* the entrusted information. For example, in the personal trust scenario, disclosing the information would permanently damage the relationship with the friend who had entrusted the information. In the workgroup scenario, disclosing would constitute a breach of the workgroup's confidence leading to an informal reprimand and a possible downgrading of one's immediate career prospects. In the national security scenario (i.e., where participants had been entrusted with classified information), a decision to disclose constituted a breach of national security. Nested within this scenario was a variant relating to the prospect of formal punishment for the breach. That is, participants could either expect the breach of national security to lead or not lead to a process where they would be formally punished.

The second factor was the *consequence of not disclosing* the entrusted information. As outlined earlier, to test *when* these consequences may motivate one to disclose, they were manipulated across three broad levels, in this case: (1) harm befalling a colleague (i.e., a colleague makes a poor work decision) (2) harm befalling a Division (i.e., a costly disruption to a major Divisional project), and (3) harm befalling DSTO as a whole (i.e., DSTO is compromised in its ability to achieve key goals) with this continuum assumed to represent levels of increasing risk. To test *for*

whom one might disclose, a number of variants were nested within these consequences relating to the participant's group/organizational affiliations. Specifically, the colleague harmed by non-disclosure was said to be either from the participant's workgroup or another workgroup, while the Division harmed was said to be either the participant's own or another Division. Also nested was a variant relating to the participant's identifiability as a 'non-discloser'. That is, participants could or could not expect to be identified by those harmed by non-disclosure if they chose not to disclose the information. After reading each disclosure dilemma, participants were asked whether they would or would not disclose the entrusted information[6].

Results indicated that for the personal trust scenario, the proportion of participants deciding to disclose partially conformed to what was expected. While the proportion of participants breaking the personal trust was greatest at the highest level of risk, that is, when non-disclosure threatened to harm DSTO globally (59%), there was no difference between the proportions disclosing for the sake of a colleague and for a Division, suggesting that this differentiation was not particularly meaningful for these participants. In all cases however, participants were more willing to breach the friend's trust when non-disclosure would harm an affiliated element compared to an unaffiliated one. That is, participants were more willing to breach the trust in order to avoid harm befalling a colleague from their own Group (49%) compared to one from another Group (34%), and to avoid harm befalling their own Division (49%) compared to another Division (34%). There were also some unexpected results. First, the prospect of being identified as a non-discloser did not lead to an increase in the number of participants disclosing as expected. Indeed, if anything, identifiability as a non-discloser resulted in a net *decrease* in the proportion of participants deciding to disclose. Second, and as mentioned above, despite the fact that the number of participants breaching the personal trust was greatest when non-disclosure threatened to harm DSTO globally, this remained less at than 60%. In other words, over 40% of participants indicated that they would not breach the trust of a friend in order to avert a major top-level failure from taking place within their organization. This pattern was reflected to some degree in the responses to the workgroup confidence scenario.

---

5. The pilot study and Study 1 contained a number of items measuring other variables. Only measures relating to the aims of this thesis are set out here.

Again, participants were far more willing to breach the workgroup confidence were non-disclosure would harm their own Division (41%) compared to when it would harm another Division (17%). However here, only 31% of participants indicated that they would breach the group confidence to prevent a major top-level failure within DSTO.

However, in the national security scenario, the number of participants indicating that they would commit a breach of national security under any of the conditions was either zero or very low. No participants indicated an intention to commit a breach of national security when non-disclosure threatened to harm a colleague's career, regardless of the colleague's shared or unshared group membership and of whether participants could expect their breach to lead to formal punishment or not. Four participants indicated an intention to breach national security when non-disclosure threatened to harm a Division, three of which when the breach would not attract formal punishment and only one for a Division other than the participant's own. When non-disclosure would harm DSTO globally, two participants indicated an intention to breach national security when such a breach attracted formal punishment, while five indicated they would do so when they could expect to evade formal punishment.

Implications

While the results of the pilot study are vaguely suggestive of the expected pattern in that the number of disclosures (i) increased as the consequences of non-disclosure grew more severe, (ii) favoured one's Divisional affiliation, and (iii) were positively influenced by an expected lack of punishment, the low frequencies obviously work against drawing any firm conclusions about this scenario. There are a number of possible reasons for the zero or near-zero disclosure rates observed across the dilemmas of the national security scenario. First, the very low proportions may be indicative of participants' desire to behave in a socially desirable way, that is, to not breach national security under any circumstances. Second, participants may not have had sufficient trust in the experimenter's assurance of anonymity, hindering their willingness to make a honest response. A series of questions as to whether one would intend to breach national security under this or that circumstance is a rather unusual

event outside of a formal security clearance briefing. Third, it is possible that the national security scenario made salient 'real-world' consequences that may stem from a breach of national security (e.g., jeopardising a planned ADF deployment). Fourth, the relative lack of *operational* experience amongst the participants (i.e., as civilians) may have encouraged a strict 'by-the book' approach to the resolution of these dilemmas. On this, despite the fact that DSTO personnel are routinely required to manage the receipt and dissemination of classified information, they are not routinely required to manage the complex array of consequences and dependencies which characterise the modern military environment, both on and off the battlefield.

In summary, the pilot study provided a valuable pre-test before embarking on a investigation involving a larger sample of ADF personnel. Generally speaking, disclosure proportions followed the contours of risk, increasing as the harm associated with non-disclosure grew progressively more severe. Further, results suggested that disclosure intentions may be moderated to some degree by the potential discloser's organizational affiliations, opening the way for including measures of identification with organizational groups and categories as predictors of prospective disclosure behaviour. Indeed, it could be argued that the affiliation which ADF personnel have with their chosen Service is likely to moderate disclosure intentions to a greater extent than that which Defence scientists have with their particular Division. Despite the low frequency of prospective disclosures in the national security scenario, the trend here suggests that the prospect of formal punishment may yet play a important role in shaping disclosure outcomes in an ADF setting. In contrast, the prospect of being identified as a non-discloser does not appear to warrant further attention as it relates to prospective breach behaviour. The lack of an effect for identifiability may be due to participants simply deferring responsibility for the harm caused by non-disclosure back to the original source of concealment, whether that be one's friend, one's workgroup or national security policy.

Hypotheses for Study 1

The question now is whether our expectations hold in an investigation of whether ADF personnel would disclose (i.e., breach national security) in order to

avoid problematic non-disclosure, and if so, when and for whom? Formally, we expect the following:-

H1: As the consequences of non-disclosure grow progressively more severe:

- the perceived importance of disclosing will increase.
- the perceived importance of not disclosing will decrease, and
- the proportion of ADF personnel deciding to disclose will increase.

H2: These expectations will be moderated by a 'Service-loyalty' effect in that:

- the perceived importance of disclosing will be higher.
- the perceived importance of not disclosing will be lower, and
- the proportion of ADF personnel deciding to disclose will be greater

when non-disclosure will harm one's own Service compared to another Service.

H1 and H2 can be depicted graphically as a step-function disclosure gradient as shown in Figure 4.1. This hypothesized gradient with its expectation of 'Service-loyalty' (H2) can be contrasted with that gradient consistent with the doctrine of Jointness (dashed line), that is, a gradient in which Service boundaries do not impact on disclosure outcomes.

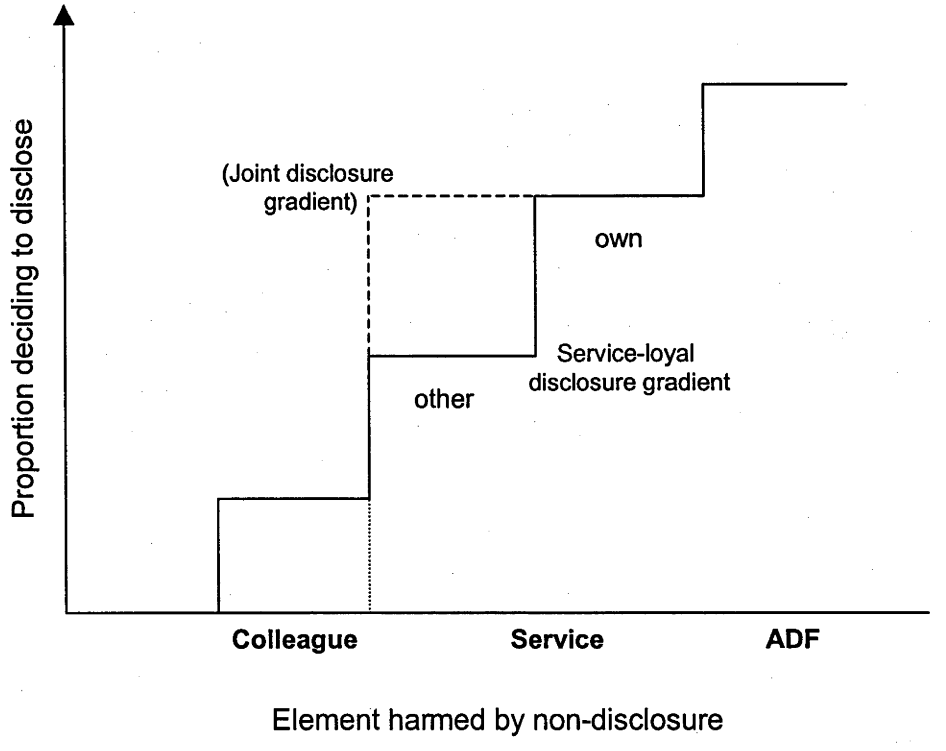


Figure 4.1 Overview of Study 1 hypotheses as a disclosure gradient.

H3: These expectations will be moderated by a formal punishment effect in that:

- the perceived importance of disclosing will be higher.
- the perceived importance of not disclosing will be lower, and
- the proportion of ADF personnel deciding to disclose will be greater

when formal punishment for disclosing is not expected compared to when it is expected.

As mentioned in Chapter 3, identification has emerged as a variable of major interest for organizational theorists working from a psychological perspective (e.g., Ashforth & Mael, 1989; Dutton, Dukerich, & Harquail, 1994; Haslam, 2004; Hogg & Terry, 2000). Organizational identification is defined in various ways, however the core of most definitions is the idea that, under certain circumstances, individuals come to perceive themselves to be 'at one' with their organization or some component of it (Ashforth & Mael, 1989; Mael & Ashforth, 1992). Specifically, the extent to which an individual identifies with various organizational categories has been considered a critical antecedent of their actual organizational behaviour (Haslam, 2004; Haslam, Eggins & Reynolds, 2003). Central to this work is the argument that the psychological processes bound up with the various organizational identities of employees underpin important organizational outcomes, including cooperation, communication, motivation, and so on (Haslam, 2004; Tyler & Blader, 2000). In light of this progress, measures of organizational identification relevant to the ADF context will be included in Study 1 as potential predictors of prospective disclosure behaviour.

Overall, measures of organizational identification are expected to be reliable predictors of prospective breach behaviour to the extent that they are related to the element harmed by non-disclosure. Thus, specific hypotheses can be devised for each element harmed by non-disclosure, as follows:

Disclosing for a colleague from another work area

Under certain conditions, an individual who identifies with a particular social group may behave positively toward members of other social groups if they perceive those other groups as sharing a superordinate goal or purpose (Haslam, 2004; Haslam et al., 2003). For example, members of a volunteer tree-planting group may behave positively toward other groups concerned with, say, the health of waterways or the reduction of air pollution, because they see these others to have a common goal, in this case, to preserve the environment. Clearly, this process depends on the absence of factors that may mitigate against the perception of a shared goal such as real or perceived competition. In assuming that such factors are unlikely to characterise the relationship between the work areas of a single military Headquarters, it is hypothesised that:

H4(a): When non-disclosure would harm a colleague from another work-area, identification with one's work area will predict a decision to disclose.

Disclosing for another service

Based on the process above, it follows that when non-disclosure would harm another Service, prospective breaches of national security could be expected to the extent that ADF personnel identify with their *own* Service. However, this is not the only identification category that may be relevant to inter-Service disclosure of this sort. Each Service belongs to the superordinate categories 'ADF' and 'Joint', yet the latter might be best described as an organizational ideology of "Jointness" (see Beaumont, 1993; Behm et al., 2001). Thus, we expect that:

H4(b): When non-disclosure would harm another Service, identification with multiple loci will predict a decision to disclose. These are (i) one's own Service, (ii) the ADF, and (iii) Jointness.

Disclosing for one's own Service

Straightforwardly, it can be hypothesized that:

H4(c): Identification with one's Service will predict a decision to disclose when non-disclosure would harm one's Service.

Disclosing for the ADF

Also straightforwardly, it can be expected that:

H4(d): Identification with the ADF will predict a decision to disclose when non-disclosure would harm the ADF.

The hypotheses above refer to prospective disclosures that constitute a breach of national security. However, and following the pilot study, two additional scenarios are to be included in Study 1 - a personal trust and a workgroup confidence scenario, in which work-relevant but unclassified information is at hand. As explained earlier, these additional scenarios serve two functions: (1) to give ADF personnel a sense of the broader research issue in a way that avoids them being initially confronted with a scenario relating to their entrustment with, and prospective handling of, classified information, and (2) to broaden the scope of the research issue in order to provide a basis for comparing the factors affecting disclosure intentions across classified and unclassified contexts. Therefore, the hypotheses outlined above apply also to the prospect of breaching a personal trust and a workgroup confidence, except H3 which specifically relates to the prospect of being formally punished for breaching national security.

Study 1

Method

Participants and design

Two-hundred and thirty-one commissioned ADF personnel participated in Study 1. This comprised 94 RAAF, 71 RAN, and 65 ARA officers (1 did not identify their Service). Participants were drawn from a number of organizations including Army, Navy and Air Force Headquarters (AHQ, NHQ, AFHQ), the Defence Materiel Organization (DMO) and Ministerial and Strategic Services Branch. The majority

(87%) were men aged between 35 and 44 years. Most (63%) were of Major-equivalent rank or below, with around a quarter (26%) of Lieutenant Colonel-equivalent rank and the remainder (11%) of Colonel-equivalent rank or above. Participants had spent an average of 20 years in the ADF and most (70%) held a TOP SECRET security clearance.

Participants read three information entrustment scenarios: (1) a personal trust scenario; (2) a workgroup confidence scenario; and (3) a national security scenario, where only the latter involved the entrustment of classified information. Participants responded to each under three conditions representing different 'elements' that would be harmed by non-disclosure, either: (1) a colleague; (2) a Service, or; (3) the ADF globally, and this was manipulated within-participants. For each scenario, a decision to disclose constituted a breach of the entrustment relationship. Within the cells of this 3 x 3 design were a number of nested variants (labels shown in italics). Nested within the national security scenario were two variants whereby disclosing either would or would not lead to an official process that revealed a crime had been committed (*punishment/no punishment*). Nested in the condition where non-disclosure harmed a Service were two variants whereby non-disclosure harmed either the participant's *own* or *another Service*. This yielded 16 disclosure dilemmas as illustrated in Figure 4.2.

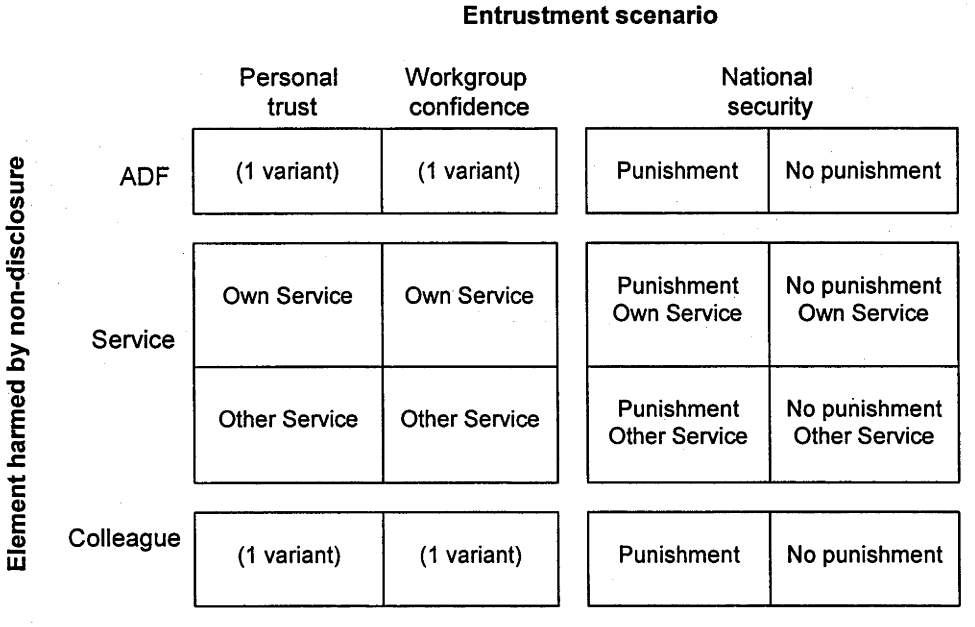


Figure 4.2 Overview of Study 1 design

Materials and procedure

The 3 entrustment scenarios read as follows:

1. Personal trust scenario

> In the course of your normal working week you meet regularly with an ADF friend to informally discuss strategic-level Defence projects. On this particular occasion, your friend shares with you some information outlining upcoming changes to the funding of certain projects. These changes would immediately interrupt a number of major projects with important force structure and capability implications. Your friend informs you that this information is reliable and trusts you not to provide the information to others.

2. Workgroup confidence scenario

> In the course of your normal work duties you are involved in the development and management of a range of strategic-level Defence projects. On this particular occasion your work area provides you with some information outlining upcoming changes to the structure and staffing of certain projects. These changes would immediately interrupt a number of major projects with important force structure and capability implications. Your work area informs you this information is reliable and you are directed not to provide the information to others outside your work area.

3. National security scenario

> In the course of your normal work duties you are privy to classified information about ADF activities. Upon receipt of official requests you provide this information to other areas of the ADF. On this particular occasion, for reasons beyond your control, no time is available for an official request to be made and instead you have been asked to provide the information unofficially. Assume that providing the information unofficially would not adversely affect any current or planned ADF operation.

For each scenario respectively, the consequences of disclosing read as follows (bracketed terms indicate wording used in different conditions):

> Providing the information to others will permanently damage the valued relationship you have established with your ADF friend who has trusted you not to disclose the information.
>
> Providing the information to others outside your work area will break the confidence it has established. This will result in you receiving an informal reprimand which will not be explicitly referred to on your annual report, but may affect your immediate career advancement prospects.
>
> Providing the information unofficially will constitute a breach of national security [and will/but will not] lead to an investigation that will reveal *prima facie* commission of an offence under the Crimes Act.

For each scenario respectively, the consequences of not disclosing read as follows (bracketed terms indicate the wording used in different conditions):

> Not providing the information to [others/others outside your work area/those making the unofficial request] will cause an ADF colleague from another work area within your Headquarters to make a bad decision that will unfairly limit their career advancements prospects.
>
> Not providing the information to [others/others outside your work area/those making the unofficial request] will result in a significant and costly disruption to the implementation of a major project belonging to [your/another] Service.
>
> Not providing the information to [others/others outside your work area/those making the unofficial request] will lead to a situation in which certain strategic and operational areas of the ADF will be severely compromised in their ability to achieve key goals, and will likely lead to an increased risk of casualties to ADF personnel.

Study questionnaires (see Appendix A) were distributed with a covering letter copied on Defence Department (DSTO) letterhead. This letter informed participants that the study was part of a research program investigating how strategic-level ADF personnel make decisions about disclosing information within the strategic Defence enterprise. It also informed participants that the research was part of a PhD program being conducted at the Australian National University, that their participation was on a voluntary basis, and that all responses would be anonymous and confidential.

Dependent Measures

For each dilemma, participants were asked to respond to three questions. The first asked participants to rate how important they believed it was for the particular entrustment relationship to be maintained (i.e., the perceived importance of not disclosing). This was measured using the following item (all bracketed phrases indicate wording used across the 3 scenarios respectively):

> In this dilemma, how important do you think it is to [maintain the trust of your ADF friend who provided you with the information?/maintain the confidence established by your work area?/**only** provide the information to those making an official request?].

The second question asked participants to rate how important they believed it was for the information to be disclosed. This was measured using the following item:

> In this dilemma, how important do you think it is to provide the information to [others?/others outside your work area?/those making the unofficial request?].

For both Questions 1 and 2, participants responded on 7-point Likert-type scales ranging from 1 (not at all) to 7 (very important). The third question asked participants to tick whether they would or would not disclose the entrusted information. This was measured using the following item:

> I [would/would not] provide the information to [others/others outside my work area/those making the unofficial request].

Along the lines proposed by Doosje, Ellemers, and Spears (1995), the extent to which participants identified with: (a) their work area, (b) their Service, (c) the ADF, and (d) Jointness, was measured with the following 3 items: (1) "I identify with [my work area/my Service/the ADF as a whole/Joint areas"]; (2) "I feel strong ties with the personnel of [my work area/my Service/the ADF as a whole/Joint personnel"]; (3) "I am committed to the aims of [my work area/my Service/the ADF as a whole/Joint aims"]. For each, responses were made on 7-point scales ranging from 1 (not at all) to 7 (a great deal).

Finally, demographic information including age, sex, rank, length of ADF tenure, and level of security-clearance level was collected. Participants were thanked for their participation and invited to make comments.

Results

Data reduction

A high degree of inter-item reliability was present between the items used to measure participants' identification with the four organizational foci. Therefore, they were collapsed to create four aggregate scales measuring participants' identification with: (1) their work-area (α=.83); (2) their Service (α=.80); (3) Jointness (α=.90); and (4) the ADF (α=.86).

Means and inter-correlations between the four identification scales are shown in Table 4.1. A relatively high degree of inter-correlation was observed between the scales measuring participants' identification with Jointness and with the ADF. Given their mean differences, and that these scales were differentially related to participants' identification with their Work area and their Service, it was decided that each was sufficiently discriminative with respect to the other. Thus, no further data reduction was performed.

Table 4.1

Means and inter-correlations for identification scales.

Scale	Mean	1	2	3	4
1. Work Area	5.70	---	.57**	.65**	.40**
2. Service	5.91		---	.46**	.61**
3. Jointness	5.09			---	.75**
4. ADF	5.37				---

** $p<.01$

Personal trust & workgroup confidence scenarios

Analysis of variance (ANOVA)

Means for the perceived importance of disclosing and not disclosing in the personal trust and workgroup confidence scenarios are summarised in Table 4.2. In both scenarios, the trend follows the hypothesized pattern, that is, as the consequences of non-disclosure grow progressively more severe, the perceived importance of disclosing increases, of not disclosing decreases, and there is a favouritism toward one's own Service *vis-à-vis* another Service. Means for the perceived importance of disclosing are generally higher in the personal trust scenario while those for the perceived importance of not disclosing are generally higher in the workgroup confidence scenario.

Table 4.2

Means and standard deviations for key dependent measures: Personal trust and workgroup confidence scenarios

	Element harmed by non-disclosure			
Perceived importance of...	Colleague	Other Service	Own Service	ADF
		Personal trust		
Disclosing	4.23_a (1.85)	4.57_b (1.88)	5.00_c (1.80)	6.35_d (1.31)
Not disclosing	5.48_a (1.60)	5.35_a (1.61)	5.17_b (1.71)	4.13_c (2.27)
		Workgroup confidence		
Disclosing	3.99_a (1.82)	4.07_a (1.93)	4.17_a (1.93)	5.98_b (1.56)
Not disclosing	5.73_a (1.31)	5.66_a (1.42)	5.63_a (1.47)	4.57_b (2.15)

Standard deviations shown in brackets.
Means not sharing subscripts differ significantly at $p<.01$ or less.

For both scenarios, scores on these items were submitted to a one-way within-subjects analysis of variance (ANOVA) comparing the four elements that could be harmed by non-disclosure (i.e., colleague, another Service, own Service, and ADF). In the personal trust scenario, a main effect was observed on the perceived importance of disclosing ($F_{(3,690)} = 164.16, p<.001, \eta^2 = 0.42$). Planned comparisons revealed that the perceived importance of disclosing was significantly higher when non-disclosure would harm the ADF compared to one's own Service ($F_{(1,230)} = 187.62, p<.001$), one's own Service compared to another Service ($F_{(1,230)} = 52.13, p<.001$), and another Service compared to a colleague ($F_{(1,230)} = 8.85, p<.01$). A main effect was also observed on the perceived importance of not disclosing ($F_{(3,690)} = 81.92, p<.001, \eta^2 = 0.26$). Planned comparisons showed that the perceived importance of not disclosing was significantly lower when non-disclosure would harm the ADF compared to one's own Service ($F_{(1,230)} = 85.85, p<.001$) and one's own Service compared to another Service ($F_{(1,230)} = 20.7, p<.001$). Thus, support was found for both H1 and H2 in this scenario.

In the workgroup confidence scenario, a main effect was observed on the perceived importance of disclosing ($F_{(3,690)} = 177.85, p<.001, \eta^2 = 0.44$). Planned comparisons revealed that the perceived importance of disclosing was significantly higher when non-disclosure would harm the ADF compared to all other conditions, with no other significant differences. A main effect was also observed on the perceived importance of not disclosing ($F_{(3,690)} = 81.21, p<.001, \eta^2 = 0.26$). Planned comparisons revealed that the perceived importance of not disclosing was significantly lower when non-disclosure would harm the ADF, again compared to all other conditions and with no other significant differences. Thus, only a marginal degree of support was found for H1 in this scenario and no support for H2.

Confidence intervals

The proportion (i.e., percentage) of participants indicating they would disclose across each of the dilemmas in the personal trust and workgroup confidence scenarios is shown in Figure 4.3. Proportions generally followed the hypothesized pattern, that is, an increase in the proportion disclosing as the consequences of non-disclosure grow progressively more severe, and higher proportions disclosing when non-disclosure will harm one's own Service compared to when it will harm another Service.

In the personal trust scenario, the proportion disclosing was significantly higher when non-disclosure would harm the ADF compared to when it would harm one's own Service (D=.32; $CI_{0.95}$ = [.382, .256]), another Service (D=.43; $CI_{0.95}$ = [.352, .484]), and a colleague (D=.48; $CI_{0.95}$ = [.411, .546])[7]. Additionally, the proportion disclosing was significantly higher when non-disclosure would harm one's own Service compared to another Service (D=.11; $CI_{0.95}$ = [.055, .142]) and a colleague (D=.16; $CI_{0.95}$ = [.103, .227]), with no other significant differences. With respect to disclosure proportions, support was found for H1 and H2 in this scenario.

6. Confidence intervals for the difference between proportions (D) were calculated using the formulae outlined by Newcombe (1998).

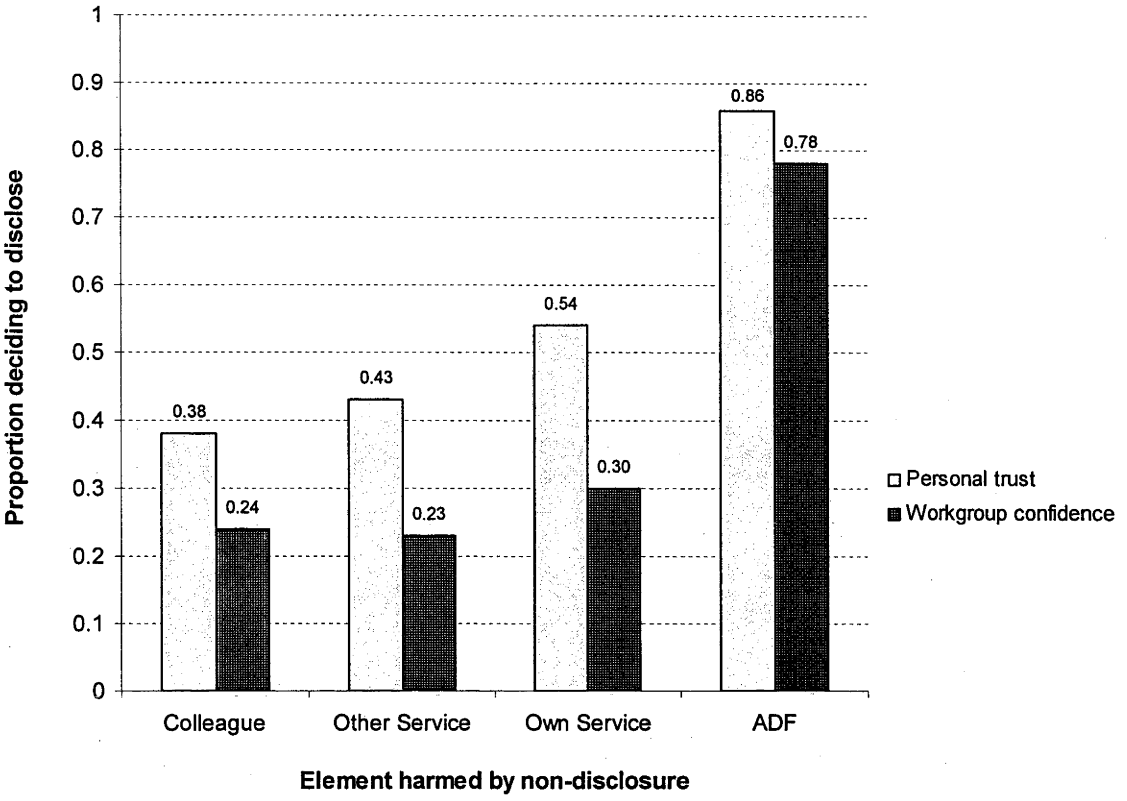


Figure 4.3 Prospective disclosure proportions: Personal trust & workgroup confidence scenarios.

In the workgroup confidence scenario, the proportion disclosing was significantly higher when non-disclosure would harm the ADF compared to when it would harm one's own Service (D=.48; $CI_{0.95}$ = [.539, .409]), another Service (D=.55; $CI_{0.95}$ = [.474, .604]) and a colleague (D=.56; $CI_{0.95}$ = [.471, .605]). Further, the proportion disclosing was significantly greater when non-disclosure would harm one's own Service compared to when it would harm another Service (D=.07; $CI_{0.95}$ = [.027, .106]), with no other significant differences. Thus while only marginal support was found for H1, strong support was found for H2 in this scenario.

Logistic regression

Logistic regression analysis was performed on a decision to disclose with the four identification scales acting as predictors. Rather than testing a full model with all four scales treated as one set of predictors, each identification scale was entered and

assessed independently. Table 4.3 shows regression statistics for each of the four scales across the dilemmas of the personal trust and workgroup confidence scenarios.

For the personal trust scenario, identification with the ADF acted as a significant predictor of a decision to disclose when non-disclosure would harm another Service, with no other significant associations observed. Thus, of the identification hypotheses, only partial support was found for H4(a) in this scenario. For the workgroup confidence scenario, identification with one's Service and with the ADF acted as a significant predictors of a decision to disclose when non-disclosure would harm another Service, with no other significant associations observed. Thus, partial support was found for H4(b). Further, identification with both one's Service and the ADF acted as a significant predictor of a decision to disclose when non-disclosure would harm one's own Service. Thus, support was found for H4(c) in this scenario.

Table 4.3

Logistic regression analysis: Personal trust and workgroup confidence scenarios

	Element harmed by non-disclosure											
	Colleague			Other Service			Own Service			ADF		
	Personal trust											
Scale	*B*	*SE B*	ß	*B*	*SE B*	ß	*B*	*SE B*	ß	*B*	*SE B*	ß
Work-area	-0.17	0.12	2.08	0.16	0.12	1.78	0.04	0.11	0.09	0.00	0.17	0.00
Service	-0.04	0.14	0.08	0.27	0.15	3.41	0.16	0.14	1.34	0.07	0.19	0.12
Jointness	-0.06	0.13	0.20	0.22	0.13	2.65	0.01	0.13	0.00	0.27	0.18	2.23
ADF	-0.03	0.11	0.07	0.45	0.13	12.51***	0.18	0.11	2.33	0.25	0.16	2.46
	Workgroup confidence											
	B	*SE B*	ß	*B*	*SE B*	ß	*B*	*SE B*	ß	*B*	*SE B*	ß
Work-area	-0.04	0.13	0.08	0.20	0.15	1.80	0.13	0.13	1.03	-0.12	0.15	0.65
Service	0.20	0.17	1.34	0.63	0.21	9.09**	0.50	0.18	7.92**	-0.11	0.17	0.39
Jointness	-0.13	0.15	0.84	0.13	0.17	0.57	-0.12	0.14	0.68	-0.02	0.16	0.01
ADF	0.22	0.14	2.52	0.71	0.18	16.28***	0.29	0.13	5.02*	0.12	0.13	0.86

* $p<.05$; ** $p<.01$; *** $p<.001$.

National security scenario

Analysis of variance (ANOVA)

Means for the perceived importance of disclosing and not disclosing in the national security scenario are summarised in Table 4.4. The trend in these means reflects the hypothesized patterns, that is, as the consequences of non-disclosure grow progressively more severe, the perceived importance of disclosing increases, the perceived importance of not disclosing decreases, and there is a favouritism toward one's own Service *vis-à-vis* another Service. Further, the perceived importance of

disclosing is generally higher in the *no punishment* condition while that of not disclosing is higher in the *punishment* condition. Compared to the previous scenarios, the perceived importance of disclosing is generally lower in the national security scenario while the perceived importance of not disclosing is generally higher.

Table 4.4

Means and standard deviations for key dependent measures; National security scenario.

	Element harmed by non-disclosure			
Perceived importance of...	Colleague	Other Service	Own Service	ADF
		Punishment		
Disclosing	2.75 (1.79)	3.02 (1.91)	3.36 (2.06)	5.32 (1.90)
Not disclosing	6.35 (1.01)	6.13 (1.40)	6.12 (1.37)	5.21 (2.05)
		No punishment		
Disclosing	3.24 (1.96)	3.59 (2.01)	4.00 (2.01)	5.43 (1.91)
Not disclosing	5.96 (1.36)	5.82 (1.52)	5.74 (1.54)	5.12 (2.01)

Note: Standard deviations shown in brackets.

Scores on these items were submitted to a 2 (punishment/no punishment) x 4 (element harmed by non-disclosure: colleague/own-Service/other-Service/ADF) mixed within/between-subjects ANOVA.

There was a main effect for the element harmed by non-disclosure on the perceived importance of disclosing to the unofficial request ($F_{(3,687)} = 204.65$ $p<.001$, $\eta^2 = 0.47$). Planned comparisons revealed that estimated marginal means on this item differed as hypothesized. Specifically, the perceived importance of disclosing was significantly higher when non-disclosure would harm the ADF ($M=5.37$) compared to one's own Service ($M=3.67$; $F_{(1,229)} = 222.55$, $p<.001$), one's own Service compared to another Service ($M=3.29$; $F_{(1,229)} = 24.34$, $p<.001$), and another Service compared to a colleague ($M=2.98$; $F_{(1,229)} = 14.02$, $p<.001$). Thus, support was forthcoming for

both H1 and H2 for this scenario. This effect was qualified by a significant interaction with participants' expectations regarding whether or not they would be formally punished for disclosing ($F_{(3,687)} = 2.57, p \leq .05$). Further analysis revealed that the perceived importance of disclosing to the unofficial request was greater in the *no punishment* condition than in the *punishment* condition across all levels of the within-subjects factor except where non-disclosure would harm the ADF. Thus, qualified support was also found for H3 in this scenario. This interaction is shown in Figure 4.4.

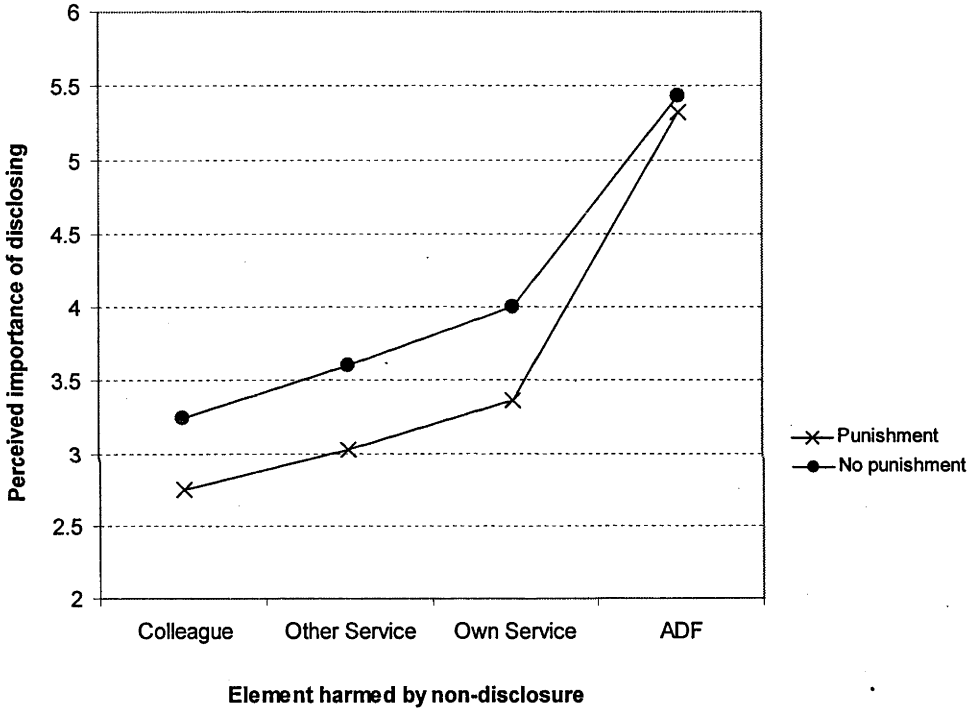


Figure 4.4 Perceived importance of disclosing as a function of element harmed by non-disclosure and consequence of breaching national security.

There was also a main effect for the element harmed by non-disclosure on the perceived importance of not disclosing ($F_{(3,687)} = 51.65, p < .001, \eta^2 = 0.18$). Planned comparisons revealed that the perceived importance of not disclosing was significantly lower when non-disclosure would harm the ADF (M=5.17) compared to when it would harm another one's own service (M=5.94; $F_{(1,229)} = 59.37$ p<.001), and when non-disclosure would harm another Service (M=5.98) compared to when it

would harm a colleague (M= 6.16; $F_{(1,229)}$ = 8.15 p<.01), with no other significant differences evident. These results provided mixed support for H1 but no support for H2.

A final main effect was observed for the between-subjects factor (*punishment/ no punishment*) on the perceived importance of disclosing ($F_{(1,229)}$ = 4.14, p<.05, η^2 = 0.02). As hypothesized, estimated marginal means on this item were higher when participants expected a decision to disclose to not lead to formal punishment (M = 4.06) compared to when formal punishment could be expected (M = 3.61), supporting H3.

Confidence intervals

The proportion (i.e., percentage) of participants indicating that they would disclose across each of the dilemmas in the national security scenario is shown in Figure 4.5. The trends generally follow the hypothesized patterns, with a higher rate of disclosing in the *no punishment* compared to the *punishment* condition and a steady increase in the proportion of participants deciding to disclose as the consequences of non-disclosure grow progressively more severe. Further, disclosure proportions are higher for when non-disclosure will harm one's own Service compared to when it will harm another Service.

For both the punishment and no punishment conditions, the proportion of participants disclosing when non-disclosure would harm the ADF was significantly higher that disclosing when it would harm one's own Service (D=.35; $CI_{0.95}$ = [.262, .435]; D=.31; $CI_{0.95}$ = [.209, .391] respectively). Further, the proportion disclosing when non-disclosure would harm one's own Service was greater than that when it would harm another Service in both the punishment (D=.03) and no punishment conditions (D=.06), however the difference only reached significance in the latter condition ($CI_{0.95}$ = [.003, .127]). Finally, the proportion disclosing when non-disclosure would harm another Service was significantly higher than that disclosing when the harm would befall a colleague in both the punishment (D=.09; $CI_{0.95}$ = [.027, .148]) and no punishment (D=.11; $CI_{0.95}$ = [.039, .185]) conditions. Thus, support was found for both H1 and H2.

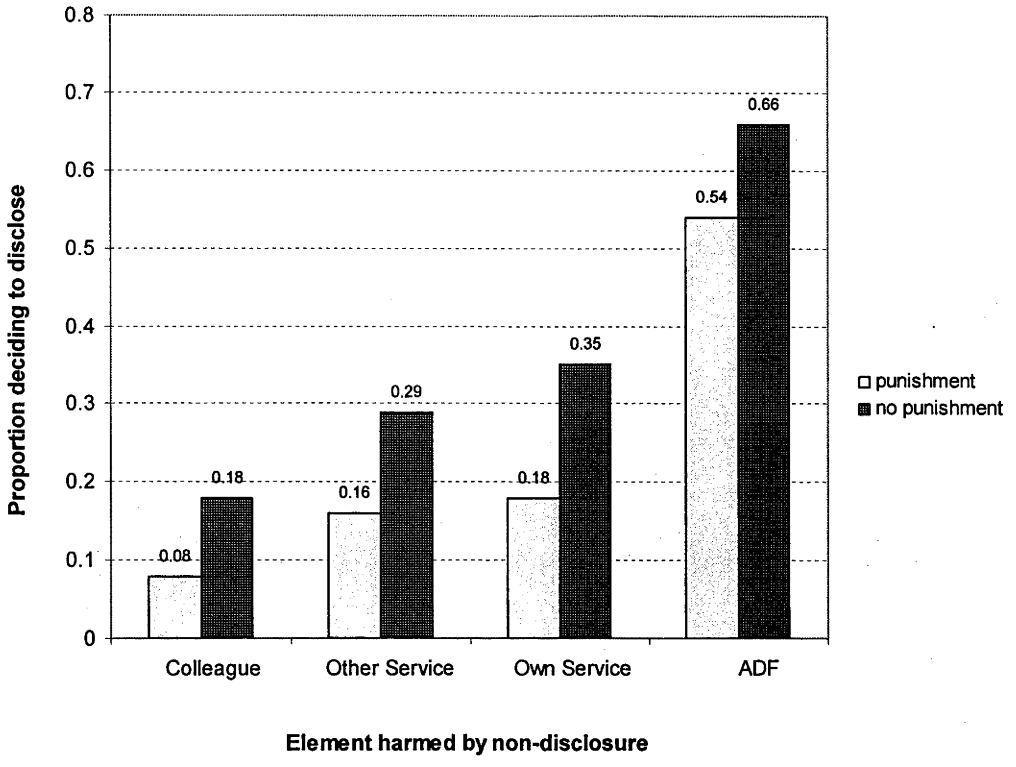


Figure 4.5 Prospective disclosure proportions: National security scenario

---

The higher rate of disclosing in the *no punishment* condition compared to the *punishment* condition was significant for those dilemmas where non-disclosure would harm a colleague (D=.11; $CI_{0.95}$ = [.015, .191]), another Service (D=.13; $CI_{0.95}$ = [.027, .242]), and one's own service (D=.26; $CI_{0.95}$ = [.052, .278]). While more participants decided to disclose in the *no-punishment* condition when non-disclosure would harm the ADF (D=.12), the difference between conditions was not significant ($CI_{0.95}$ = [-.237, -.012]), reflecting the pattern shown in Figure 4.5. Thus, qualified support was found for H3.

Logistic Regression

Logistic regression analysis was performed on a decision to disclose (i.e., breach national security) with the four identification scales acting as predictors. Again, rather than testing a full model with all four identification scales treated as one set of predictors, each identification scale was entered and assessed independently of the others. Tables 4.5 shows the regression statistics for each of the four scales across

the dilemmas of the national security scenario for both the punishment and no punishment conditions. Identification with the ADF acted as a significant predictor of a decision to disclose when non-disclosure would harm another Service, yet only in the punishment condition, with no other significant associations evident. Thus, only marginal support was found for H4(b) of all the identification hypotheses.

Table 4.5

Logistic regression analysis: National security scenario

	Element harmed by non-disclosure											
	Colleague			Other Service			Own Service			ADF		
	Punishment											
Scale	*B*	*SE B*	ß	*B*	*SE B*	ß	*B*	*SE B*	ß	*B*	*SE B*	ß
Work-area	0.16	0.34	0.23	0.42	0.29	2.11	0.58	0.30	3.79	0.34	0.17	3.77
Service	0.29	0.41	0.49	0.48	0.32	2.21	0.37	0.28	1.69	0.17	0.18	0.91
Jointness	-0.19	0.31	0.37	0.01	0.28	0.00	-0.09	0.22	0.16	0.01	0.18	0.00
ADF	0.12	0.31	0.16	0.60	0.29	4.32*	0.24	0.22	1.16	0.18	0.16	1.33
	No punishment											
Scale	*B*	*SE B*	ß	*B*	*SE B*	ß	*B*	*SE B*	ß	*B*	*SE B*	ß
Work-area	-0.19	0.20	0.83	-0.04	0.18	0.05	-0.33	0.17	3.62	-0.28	0.19	2.10
Service	-0.38	0.28	1.93	-0.19	0.23	0.62	-0.15	0.23	0.44	-0.35	0.24	2.08
Jointness	-0.27	0.25	1.71	-0.19	0.21	0.83	-0.37	0.21	3.33	-0.23	0.21	1.20
ADF	-0.02	0.22	0.01	0.03	0.18	0.03	0.01	0.17	0.00	-0.25	0.18	1.97

* $p<.05$

Discussion

Our first hypothesis (H1) was that the proportion of participants indicating that they would breach the conditions of entrustment would increase as the consequences of non-disclosure grew progressively more severe. To test this, we manipulated the locus of harm associated with non-disclosure of the information. Specifically, non-

disclosure harmed either a colleague, a Service, or the ADF globally. We reasoned that *in this order*, these consequences represented a continuum along which the effects of non-disclosure would be perceived to grow progressively more severe. In the national security scenario, the findings showed that the perceived importance of disclosing the classified information increased, and of not disclosing decreased, with each step along the continuum. Further, results showed that the proportion of participants deciding to disclose followed the hypothesized pattern. As a result, we found support for H1.

Partial support for H1 was also forthcoming in the workgroup confidence and personal trust scenarios. Here, participants generally perceived the maintenance of the entrustment to be less important and disclosing to be more important, each step along the continuum and again rates of prospective breach behaviour generally followed the hypothesized pattern. Yet, these latter forms of entrustment appeared to evoke a somewhat less discriminating response from participants than did the national security scenario. While the proportion disclosing was greatest when non-disclosure threatened to harm the ADF, there was a tendency to equate the colleague and the other Service as loci of harm on the two perceived importance variables and indications of prospective breach behaviour (this trend was also evident in pilot study). This suggests that participants were more discriminating in their decision-making about when they might breach national security compared to when they might breach less formal types of entrustment.

Interestingly, the proportion of participants indicating they would disclose to avoid harm befalling the ADF never reached 100% in any of the three scenarios. This is particularly surprising given that this consequence also invoked the risk of ADF casualties. Specifically, when disclosing would constitute a breach of national security and lead to a process of formal punishment, only around half the participants sampled indicated they would disclose to avoid such consequences. This increased to two-thirds when the threat of punishment was lifted. While disclosure proportions in this condition were somewhat higher in the personal trust (86%) and workgroup confidence (78%) scenarios, it cannot be concluded that the threat of a major organizational failure (which in this case includes the risk of casualties) is sufficient to *guarantee* disclosure of entrusted information, classified or otherwise. In other

words, there is likely to remain a component that will not breach any form of trust under any circumstances. A sense of 'flexibility' about when disclosure is and is not justified according to the official rules was neatly captured by another participant:

> Only 'pecker-heads' retain information for purely 'security clearance' reasons. Only fools release information to everyone with a need (read 'desire') to know. (participant 19).

Our second hypothesis (H2) was that when non-disclosure would have a negative impact on a Service, participants' disclosure behaviour would be moderated according to whether they were affiliated with that Service or not. That is, we hypothesised a 'Service-loyalty effect' whereby participants would favour their own Service over another Service in terms of their willingness to breach national security and their perceptions about the importance of doing so. While participants did indeed perceive the importance of disclosing to avoid harm befalling their own Service to be greater than that for another Service, this was not the case with respect to their perceptions about the importance of not disclosing. That is, the perceived importance of maintaining national security remained steady across the own/other Service factor while that of disclosing varied according to the Service affected, suggesting that the apparent willingness of participants to breach national security is not inversely rated to their beliefs about the need to maintain national security as a whole. This partial level of support for H2 also extended to the proportions of participants indicating that they would disclose the information to the unofficial request. Specifically, no Service-loyalty effect was evident in terms of participants' prospective breaches of national security when participants could expect to receive formal punishment. When there was an expectation that one would evade formal punishment, the proportion of participants disclosing for their own Service was greater than that disclosing for another Service, however the difference in the proportions here was low (D=.06). Thus, we might conclude that if Service-loyalty is present in the context of problematic non-disclosure of classified information, it remains weak and is likely to be quashed by expectations of being formally punished. Hence, only partial support can be claimed here for H2.

Stronger support for H2 was forthcoming in the personal trust scenario. Here, significant differences between own/other Service conditions in the hypothesized direction emerged on both the perceived importance of disclosing and not disclosing. Further, there was a larger (D=.11) difference between the proportion deciding to disclose for the benefit of their own Service and another Service. In the workgroup confidence scenario however, the Service-loyalty effect emerged only in terms of participants' decisions to disclose (D=.06), not on their perceptions of how important it is to disclose and not disclose. It is possible that this reflects the formal and directive nature of the entrustment instructions in the workgroup confidence scenario.

Our third hypothesis (H3) was that the proportion of participants deciding to breach national security would be greater when they could expect to evade formal punishment compared to when formal punishment was expected. To this end, we manipulated whether a decision to disclose the classified information to an unofficial request would or would not lead to a formal process that revealed a criminal offence had been committed. The findings showed that the proportion of participants disclosing was significantly greater when they could expect to evade formal punishment for all dilemmas except where non-disclosure harmed the ADF and threatened casualties. More specifically, when the prospect of formal punishment was lifted, the proportion of participants deciding to breach national security increased by around 100% for each of these dilemmas. That the expected punishment manipulation had no significant impact on disclosure proportions when non-disclosure harmed the ADF and threatened casualties suggests that personal consequences associated with one's breach behaviour are superseded and/or rendered largely irrelevant when non-disclosure will have potentially catastrophic consequences. However, and as mentioned above, this reasoning is only relevant to those participants who decide to disclose and accept the potential costs of doing so - other factors are needed to explain why not all participants disclose in the face of such a potential disaster. The effect of the manipulation was also evident in participants' ratings of the importance of disclosing to the unofficial request. That is, the perceived importance of disclosing was higher when punishment was not expected compared to when it was. However, this was not the case with respect to the perceived importance of not disclosing (i.e., maintaining national security) which did not vary across the manipulation. This is consistent with our earlier finding that the perceived importance

of not breaching national security policy did not vary across the own/other Service manipulation. This further supports the idea that breach behaviour in the domain of national security that is brought about by situational demands does not necessarily involve changes in the discloser's beliefs about the importance of maintaining national security policy. Overall, strong support was found for H3.

Our final set of hypotheses, H4(a)-(d), concerned the predictive ability of participant identification with various organizational groups and categories. Specifically, measures of organizational identification were expected to be reliable predictors of prospective breach behaviour to the extent that they were related to the element harmed by non-disclosure. H4(a) held that identification with one's work area would predict participants' decision to breach conditions of entrustment when harm would befall a colleague from another work area. However, we found no support for this hypothesis. Specifically, results indicated that this level of identification did not predict disclosing in any scenario. One possibility for this lack of association may stem from the perceived nature of the relations between work-areas in the ADF. Specifically, it is possible that intergroup relations in this context are characterised more by competition than cooperation. Accordingly, participants may not perceive (or value) any sense of 'us' which encompasses their own and other work-areas. A second possibility is that such conditions *were* present, but were not of sufficient magnitude to motivate participants to incur the personal costs associated with disclosing, leaving good intentions on the part of the potential discloser just that.

H4(b) held that a number of identification measures would reliably predict a decision to disclose when non-disclosure would harm another Service. These included participants' identification with the ADF, their own Service, and the notion of Jointness. Findings confirmed the first of these associations in that identification with the ADF reliably predicted disclosures for another Service, not only in the national security scenario (when punishment could be expected) but also in the personal trust and workgroup confidence scenarios. One possible reason why this association emerged only in the punishment and not the no-punishment condition is that identification with an organization may become increasingly important when one must show (i.e., justify) that what appears to be anti-organizational behaviour on their part is actually pro-organizational behaviour. Identification with one's Service also

reliably predicted prospective breach behaviour for another Service in the workgroup confidence domain. Given the focus of this scenario on members of one's immediate workgroup, it is possible that identification with one's Service was more relevant in this domain than in the other two domains. However, identification with Jointness did not reliably predict disclosing when non-disclosure would harm another Service in any of the scenarios. This is intriguing given that the ideology of Jointness relates explicitly to inter-Service cooperation and is organizationally superordinate like the category 'ADF'. Why did identification with the ADF prove to be a successful predictor of inter-Service disclosure but not identification with Jointness? Part of the answer may lie in the *content* of these specific identifications and how they differ. One issue that has gained attention in this respect concerns the impact of Jointness on the distinctiveness of the Services. It has been argued that the Jointness ideology may undermine the distinctiveness of the individual Services by eroding traditional single Service roles, values, and traditions (Trainor, 1993-4; see also Cropsey, 1993; Fautua, 2000). Hence, is possible that Jointness constitutes, at least for some participants, a threat to the distinctiveness of their Service, a claim which cannot be plausibly upheld with respect to the 'ADF' category. In short, only partial support can be claimed for H4(b).

H4(c) maintained that participants' identification with their own Service would predict prospective breach behaviour when non-disclosure threatened their Service. Findings showed that this was indeed the case in the workgroup confidence scenario, but not in the personal trust or national security scenarios. As was suggested above, it is possible that the focus of the workgroup confidence scenario on one's immediate workgroup meant that participants' identification with their Service was more relevant to their responses in this domain than in the other domains. Thus, only marginal support can be claimed for H4(c).

Finally, H4(d) held that participants' identification with the ADF would predict their prospective breach behaviour when non-disclosure threatened the ADF globally. Findings showed however, that this association was not present in any of the entrustment scenarios. One explanation for this may lie in the severity of the consequences of this condition, specifically, the prospect of non-disclosure increasing the risk of ADF casualties. It is possible that the extent to which one identifies with

an organization is largely irrelevant to their behaviour in the face of catastrophe that may involve the loss of life. That is, problematic non-disclosure of such a magnitude calls for a particular response (i.e., disclosing) irrespective of one's identification with the organization. Another possibility is that such behaviour does draw on identity-related concerns but not those deriving from organizational categories and groups, for example, one's identification with humanity. Another possibility is that Service identity rather than ADF identity remains the most salient amongst this particular sample of ADF personnel. As one participant remarked at the end of the questionnaire: "I am Army first, ADF second" (participant 100).

Some final insights can also be gained *vis-à-vis* the extent to which the factors affecting the disclosure of classified information also affect the disclosure of work-relevant but unclassified information. For one, rates of prospective disclosure behaviour were generally highest in the personal trust domain and lowest in the domain of national security. Furthermore, participants appeared to be more discriminating in their decision-making when their disclosures would constitute a breach of national security compared to when it would constitute a breach of personal trust or a work group confidence. Rates of disclosure in the national security scenario were lower when non-disclosure would harm a colleague compared to a Service, and these latter rates were lower than those when non-disclosure would harm the ADF at large. However, in the two unclassified scenarios, less difference was evident in this regard especially when disclosing would harm a colleague and a Service. Having said this, participants appeared to be more discriminating in these two scenarios with respect to a particular issue, that is, the extent to which they would favour their own Service over another Service in terms of their prospective disclosure behaviour.

General summary and conclusions

This chapter marks the beginning of our empirical investigation into the factors unpinning the disclosure of classified information in the ADF. Specifically, we sought to address, in relatively broad detail, the question of when and for whom ADF personnel will breach the formal rules in order to avert problematic non-disclosure of classified information. The path taken to answer this question was largely exploratory in nature. It was guided, for the most part, by the disclosure

literature reviewed in Chapter 3. It was also theoretically pluralistic in nature, in that our hypotheses were not bound by one explanatory framework, but were drawn from many.

In its essence then, Study 1 is a demonstration of how breach behaviour in the domain of national security varies within a set of broad scope conditions. When non-disclosure would likely bring about catastrophe, little room exists for anything other than breaches of national security. However, when it has relatively local consequences, only a small proportion of personnel will breach national security. Furthermore, when one can expect with all certainty to be punished, they will breach national security to a far less extent than when they can expect any such disclosures to remain, at least formally, unobserved.

Yet, it is when non-disclosure would have what might be termed 'mid-range' consequences for the Services that the most important results emerge. Here, the proportion of participants deciding to disclose lies mid way between that when non-disclosure ensures catastrophe and that when non-disclosure will have relatively local consequences. However, the importance of these results stems from two interrelated reasons. The first is that it is in this realm where the bulk of *actual* disclosure activity involving classified information is likely to occur. That is, the disclosure of classified information will more frequently have mid-level and Service-relevant consequences, than it will have consequences that are catastrophic for the organization as a whole or for one particular member. The second reason is that 'appropriate' disclosure of classified information across Service boundaries is simply critical to the effectiveness of the ADF in both war and peacetime, a fact that underlies the organizational ideology and doctrine of Jointness and a fact which is at odds with the observation of a robust Service-loyalty effect, that is, a tendency to favour one's own Service over another in prospective disclosure behaviour.

What do these results mean for the remainder of the research program? Our goal must now be to move beyond exploratory research as to when and for whom ADF personnel will breach national security so as to avoid problematic non-disclosure. Specifically, we must move toward a more focused and theoretical understanding of the psychology that underpins the disclosure of classified

information in the ADF. In this respect, we must examine the Service-loyalty effect and the emphasis it places on the inter-Service context within which the disclosure of classified information takes place. Accordingly, a tighter focus on *intergroup* theories, such as social identity (Tajfel & Turner, 1979) and self-categorization (Turner, 1985; Turner et al., 1987) theories is appropriate to bring to the research issue at this point, thus going beyond the general notion of organizational identification discussed so far. At one level, the measures of identification included in Study 1 can be seen to have yielded mixed findings with respect to predicting prospective breach behaviour. However, they also provided the first glimpse of theoretical insight into the psychological processes that may underpin the disclosure of classified information in this context. Taken together, this mix of findings necessitates further analysis from a theoretical framework that is both relevant to an intergroup context and appreciative of the psychological processes underpinning organizational identity. This is provided by what has become known as the 'social identity perspective', a broad theoretical framework comprised of social identity theory and self-categorization theory.

CHAPTER 5

THE SOCIAL IDENTITY PERSPECTIVE:

TWO HYPOTHESES OF PROBLEMATIC NON-DISCLOSURE

Introduction

The aim of Chapter 4 was to gain an initial and broad insight into the psychology underlying problematic non-disclosure of classified information in an ADF setting. Informed by the work dealing with problematic non-disclosure in the domain of confidentiality, we posed a set of simple questions that centred around the factors of risk and group affiliation. Will ADF personnel breach the formal rules regarding access to classified information in order to avert negative consequences associated with non-disclosure? If so, when and for whom? To this end, we manipulated the element harmed by non-disclosure across three levels: a colleague, a Service, and the ADF globally (where the latter included the risk of ADF casualties). We also manipulated whether the Service harmed was the participant's own or not, and whether participants could expect any breach of national security to lead them to be formally punished or not.

The findings of Study 1 produced the broad insights desired, insights that in many but not all respects accorded with what was expected. Results showed that as the harm associated with non-disclosure moved from relatively local to relatively global levels, personnel became increasingly more willing to breach national security by disclosing the information in an unofficial capacity. Furthermore, they were significantly more willing to do so when they could expect their breach to not lead to formal punishment compared to when formal punishment was an inevitability. While these findings speak to the moderating role of risk, perhaps the most important finding at this point is that which speaks to the moderating role of group affiliation. Here, we found that ADF personnel were more willing to commit breaches (at least prospectively) when non-disclosure would harm their own Service compared to when it would harm another Service. Indeed, perceptions of the *importance* of disclosing followed the pattern of what we have termed 'Service-loyalty'. Albeit in the unusual

circumstances created in Study 1, the suggestion that problematic non-disclosure of classified information in the ADF might surface around its Service boundaries is particularly important for two reasons. First, it sits uncomfortably with the dominant ideology of Jointness, an ideology that promotes cooperation amongst the Services and seeks to ensure that Service boundaries, in and of themselves, do not impede the realisation of the ADF's capability. Second, the Service-loyalty effect, along with the findings suggesting that people's identifications might be involved in their disclosure behaviour, draws attention to a theoretical perspective that may be useful in gaining a deeper understanding of the psychology of problematic non-disclosure as it might apply to classified information in an ADF context – the social identity perspective.

The social identity perspective is comprised of the hypotheses and arguments of social identity theory (Tajfel & Turner, 1979) and self-categorization theory (Turner, 1985; Turner et al., 1987). Fundamental to the perspective as a whole is the idea that people perceive and respond to the social world in a qualitatively different way when they view themselves as members of a group than as individuals (Turner, 1999; Turner & Haslam, 2001). One's group memberships include, of course, those of *organizational* categories and groups (Ashforth & Mael, 1989) and for that reason the perspective has been influential in providing an understanding of not only the psychological foundations of issues like prejudice and stereotyping (see McGarty, Yzerbyt, & Spears; 2002, Oakes, Haslam, & Turner, 1994) but also of many organizational phenomena such as leadership, negotiation, and motivation (Haslam, 2004; Hogg & Terry, 2000). The social identity perspective is of particular relevance here because it originates from work seeking to explain the psychological processes involved in a phenomenon that bears a remarkable resemblance to what we have termed the 'Service-loyalty effect'. Specifically, the social identity perspective grew from a period of intense theoretical and empirical work that provided a psychological explanation of *ingroup favouritism*, that is, the tendency for people to favour their own group over other groups in some way, whether that be in terms of their behaviours, perceptions, or attitudes (Turner, 1981a).

The aim of this chapter is to review the social identity perspective with particular regard as to how it might explain the psychology of problematic non-disclosure in the ADF context. More specifically, the original focus of the perspective

on the psychology of ingroup favouritism suggests that it may be well placed to explain when problematic non-disclosure is likely to surface around Service boundaries. The chapter begins therefore by reviewing the social identity explanation of ingroup group favouritism, work that has been conducted largely within the tradition of social identity theory (Tajfel & Turner, 1979). Subsequently, a brief review is made of the relevant concepts and ideas reconceptualized by self-categorization theory (Turner, 1985; Turner et al., 1987). We then devise two general hypotheses of non-disclosure that draw upon these social identity processes.

Ingroup favouritism: A social identity perspective

Ingroup favouritism[8], the tendency for people to favour their own group over some relevant comparison group, is one of the most robust findings across social psychological literature (Jetten, Spears, & Manstead, 1999; Mullen, Brown, & Smith, 1992). As alluded to above, results reported in both the pilot study and Study 1 can be seen as instances of ingroup favouritism. With respect to Study 1, ADF personnel were Service-loyal in both their disclosure intentions and perceptions in each entrustment domain regardless of whether a decision to disclose breached a friend's trust, a workplace confidence, or national security policy. Strictly speaking, ingroup favouritism expressed in behavioural terms (or prospective behaviour) is known as *intergroup discrimination*. That which manifests as people's perceptions or attitudes (e.g., believing that one's group is of a higher status than another) is known as *intergroup differentiation* (Turner, 1981a). Clearly, both these concepts are intertwined and central to many phenomena, most notably social conflict. While the focus of social identity theory (Tajfel & Turner, 1979) has tended to remain on intergroup relations and social conflict in stratified societies, the theory began as an attempt to explain the emergence of ingroup favouritism in what cam to be known as the 'minimal group' studies. Indeed, it is this analysis that constitutes the theory's 'psychological core' (Turner, 1999).

---

7. The terms ingroup favouritism and ingroup bias are often used synonymously, a practice which has led to some confusion (see Turner & Reynolds, 2001). For our purposes, only the former term is used.

The minimal group studies

The broad aim of the minimal groups studies was to determine whether *social categorization*, that is, the cognitive act of categorizing people into different groups, was sufficient to evoke ingroup favouritism, or more accurately, intergroup discrimination (Tajfel & Turner, 1979). These studies typically had two phases (for an overview see Tajfel, 1970). The first phase served to isolate social categorization from other variables usually associated with intergroup discrimination, such as a conflict of interest or previous intergroup hostility. To this end, participants were categorized into two groups on the basis of some trivial criteria, for example, whether they preferred the paintings of Klee or Kandinsky or whether they were "under-" or "over-estimators" in terms of their ability to estimate the number of dots on a projected screen. Participants were not told of the group identity of each other, nor were they permitted to interact with each other. As a result, the groups were thought to be 'psychologically minimal', existing only as a social categorizations within the minds of participants.

The second phase assessed the impact of this social categorization on intergroup behaviour. In isolation, each participant was set a task that required them to distribute an amount of money between two other participants. These recipients were identified only by an arbitrary code number and their group membership (e.g., 'Member No. 74 of Klee group'). One recipient was always a member of the group to which the participant also belonged (the 'ingroup' member) while the other was a member of the alternative group (the 'outgroup' member). The actual distribution decision was to be made in accordance with a set of matrices of which their were various distribution 'strategies' embedded within. For instance, the distribution could represent: (i) the greatest *common* benefit to the two recipients (Maximum Joint Payoff); (ii) the greatest benefit to the ingroup member (Maximum Ingroup Profit); (iii) the greatest difference between the benefit awarded to the two recipients in favour of the 'ingroup' member (Maximum Difference); or (iv) an equal benefit being awarded to the two recipients (Fairness).

The highly reliable finding of the minimal group studies was one of ingroup favouritism, that is, participants awarded greater amounts of money to members of

their own group than to members of the alternative group (Tajfel, 1970; Turner, 1978a, 1999; see also Turner & Bourhis, 1996). Yet, when they had a choice between maximising the amount awarded to ingroup members (Maximum Ingroup Profit) and maximising the *difference* in what was awarded to the two recipients in favour of the ingroup member (Maximum Difference), it was the latter strategy that was favoured (Turner, 1975, 1978a). Put simply, when given the chance, participants adopted a strategy of deliberate discrimination against outgroup members, even though doing so lessened the amount of money awarded to ingroup members (Turner, 1975, 1981a). Hence, *relative* ingroup favouritism was perceived to be more important than *absolute* ingroup favouritism, or as Turner (1978b) stated, participants wanted to see their group "*win* rather than gain" (p. 102).

Tajfel and colleagues argued that the intergroup discrimination observed in the minimal group paradigm reflected, at a fundamental level, participant acceptance or 'internalization' of the social categorization provided as an aspect of their *self-concept* (Tajfel, 1972; Tajfel, Flament, Billig, & Bundy, 1971; see also Turner, 1978a). Doing so, they maintained, brought psychological structure and meaning to an otherwise barren social context. Furthermore, acceptance of the experimenter-imposed categorization also provided participants with an identity (defined in group rather than personal terms) that could make a positive contribution to the participant's view of themselves. In the context of the minimal group situation, self-enhancement was possible on only one dimension, that is, the relative distribution of money between ingroup and outgroup members (Turner, 1978).

Positive social identity: A cognitive-motivational analysis

Amongst other things, social identity theory holds that an individual's view of him- or herself is constituted, in part, by their membership of certain social groups or categories (Tajfel, 1978). More specifically, an individual's *social identity* is defined as "the individual's knowledge that he [or she] belongs to certain social groups together with some emotional and value significance to him [or her] of this group membership" (Tajfel, 1972, p. 31). As mentioned in Chapter 4, social identities in the ADF may form around various organizational groupings and categories, for instance, one's Service (e.g., 'we soldiers, sailors, airmen'), one's work-area (e.g., 'we pilots')

or one's membership of the ADF at large ('we ADF personnel'). Hence, the concept of social identity is different to that of *personal identity*, that is, a self-definition based on the knowledge one has of themselves as an individual with idiosyncratic attributes, qualities and traits (see Turner, 1982). Put another way, a social identity is a 'we' definition of oneself, rather than a 'me' definition of oneself.

Just as people are presumed to want to be evaluated positively as unique individuals (see Festinger, 1954), social identity theory maintains that people also have an inherent psychological desire to be evaluated positively in terms of their *group memberships* (Tajfel, 1978; Tajfel & Turner, 1979; Turner, 1999). Put another way, people have a need for positive regard in terms of their social identities. Hence, when an individual feels as though a particular social identity contributes positively to how they view themselves, they could be expected to do things that maintain and/or enhance this situation. For example, Army personnel who perceive that their membership of the Army makes a positive contribution to 'who they are' could be expected to remain a member of the Army for some time, and work to protect and promote its interests. Alternatively, when an individual feels as though a particular social identity makes a *negative* contribution to their self-definition, social identity theory holds that they could be expected to do things to alleviate this situation. For example, if our Army personnel felt ashamed of belonging to the Army or perceived it to reflect low status, they may leave the Army (if possible), engage in various types of activities designed to promote a positive change (e.g., mount a campaign to increase the respectability of the Army), or cognitively reinterpret attributes of the Army so that negative features become positive features (e.g., strict discipline builds character and leadership ability; Tajfel, 1978; Tajfel & Turner, 1979).

Whether the aim is creation, maintenance, or enhancement of a positive social identity, social identity theory holds that the process is *comparative* in nature (Tajfel, 1978; Tajfel & Turner, 1979; Turner, 1975; Turner & Brown, 1978). Specifically, a positive social identity is gained through a process of favourable comparison of one's own group (i.e., from which the social identity is derived) against other relevant groups, as suggested by Tajfel (1978) below:

> The characteristics of one's group as a whole (such as its status, its richness or poverty, its skin colour, or its ability to reach its aim) achieve most of their significance in relation to perceived differences from other groups and the value connotations of these differences...the definition of a group (national, racial or any other) makes no sense unless there are other groups around (p. 66).

The theory holds that the relevance of another group for comparison in this respect varies according to the social context. That is, favourable comparisons against a particular group may be very important under some circumstances and less important under others. For example, in some situations, establishing or maintaining one's social identity as a member of the RAAF may depend on making a favourable comparison of the RAAF against, say, a civilian airline (e.g., "we fly in combat, they do not"). In other situations however, establishing or maintaining a social identity as a member of the RAAF may entail positive comparisons made against the RAN or the ARA. Just which group becomes the basis for comparison or 'relevant outgroup' will depend on the prevailing circumstances. Civilian airlines may emerge as the relevant outgroup in a situation where, for example, RAAF personnel are told that "all aviation organizations are the same". The RAN or the ARA may emerge as the relevant outgroup in a situation where RAAF personnel are told they are no different to other members of the ADF. Either way, the achievement, maintenance, or enhancement of a positive social identity depends on one's social group remaining *positively distinct* from relevant outgroups (Brewer, 1981; Brown, 1978; Mullen et al., 1992; Tajfel, 1978; Tajfel & Turner, 1979).

The process described above constitutes a sequence of social categorization–social identity–social comparison–positive ingroup distinctiveness/ingroup favouritism (Tajfel, 1978; Turner, 1999). In the context of social identity theory, this sequence constitutes a cognitive-motivational analysis of the process producing a need for positive social identity, and grew out of the desire to make sense of the intergroup discrimination observed in the minimal group studies. It constitutes the core psychological hypothesis of social identity theory, namely:

> ...that social comparisons between groups which are relevant to an evaluation of one's social identity produce pressures for intergroup differentiation to achieve a positive self-evaluation in terms of that identity (Turner, 1999, p. 8).

This is not to say that ingroup favouritism and intergroup discrimination are to be understood as *inevitable* outcomes of social identification (McGarty, 2001; Turner & Reynolds, 2001). As alluded to earlier, in reality (i.e., outside of the minimal group paradigm) the process is situated within the context of real-life intergroup relations and whether an individual responds to identity-related issues with ingroup favouritism will depend not only on the strength of their identification with the relevant group or category (Ellemers, Spears, and Doosje, 1999) but their location in, and perception of the prevailing social structure. That is, whether or not they perceive it to be possible to move from one's current group to another groups that may offer higher status (Tajfel & Turner, 1979). Yet, the basic hypothesis is that many forms of ingroup favouritism represent intergroup discrimination and differentiation resulting from social comparison processes. Before turning to how this basic hypothesis might explain the psychology of problematic non-disclosure of classified information in the ADF, it will be necessary to briefly consider how some of the ideas presented above have been continued more recently by self-categorization theory (Turner, 1985; Turner et al., 1987).

Self-categorization theory

As outlined above, an individual's social identity is that part of their *self*-definition that derives from their membership of social groups or categories (Tajfel, 1972; Tajfel & Turner, 1979). The emphasis that social identity theory placed on the notion of the 'self' was further developed by self-categorization theory (Turner, 1985; Turner et al., 1987). According to this theory, the self is categorized in much the same way as natural entities in the environment. So, for example, just as a chair can be categorized on the basis of its perceived similarity to other chairs and its difference to another class of stimuli (e.g., tables), so too can the self be categorized on the basis of *its* perceived similarities and differences with respect to other stimuli, in this case, other people. Unlike the categorization of natural stimuli however, the role of self-categorization is not to determine 'What is that thing?' (Bruner, 1957). Instead, categorization of the self serves to situate the individual psychologically in the social context (Oakes et al., 1994; Turner et al., 1987). In other words, self-categorization provides the individual with an answer to the question 'Who am I?' in a given

situation. Seeing oneself as a member of a particular ingroup then represents a self-categorization at the social rather than an individual level of identity (Turner, 1991).

One important implication of this idea is that the answer to 'Who am I?' will vary with the prevailing social context (Turner et al., 1987). As a result, self-categorization theory maintains that the self is a *dynamic process* rather than a fixed cognitive structure (Onorato & Turner, 2001, 2002; Turner, Oakes, Haslam, & McGarty, 1994; Turner & Onorato, 1999). It is assumed that, like 'natural' categories, self-categories exist at different *levels of abstraction* with higher levels being the more inclusive than lower levels (Turner et al., 1987). For example, an individual may perceive themselves as an Australian, an ADF officer, an RAAF officer, or "me" with each respective self-category being less inclusive than the next. According to self-categorization theory, no one self-category is more real or inherently fundamental to a person than any other (Haslam, 2004). Rather, the self-category that is psychologically salient (i.e., cognitively activated) at a given point in time is the result of an interaction between an individual's perception of the prevailing social context and certain psychological properties (Turner et al., 1987).

Specifically, self-category salience is expected to vary lawfully in accordance with two general principles. The first is known as 'perceiver readiness' (or 'relative accessibility') and refers to how 'ready' the individual is to categorize themselves in terms of that self-category (Oakes, 1987; Turner et al., 1987). This readiness is determined by a number of factors including the extent to which the individual identifies with the category, their prior experience and their current values, motives, goals, and expectations. So, for example, the self-category 'RAAF officer' may be relatively accessible for the person who identifies strongly with their membership of this category and perceives their current goals in terms of this category. The second principle concerns the extent to which the self-category 'fits' the perceiver's perception of the prevailing social context (Oakes, 1987; Oakes et al., 1994; Turner et al., 1987). In this respect, self-category salience depends on the extent to which *within-category* differences are perceived to be less than *between-category* differences ('comparative fit'). So, for example, in the context of a meeting between RAAF, RAN and ARA officers about which Service should carry the burden of budget cuts, officers would be likely to self-categorize in terms of their chosen Service because in

this competitive context, they would be likely to perceive the differences amongst their Service colleagues to be less than those between personnel of different Services. Yet, if the prevailing social context changed dramatically, say if our RAAF, RAN, and ARA personnel were airlifted into a major military operation involving US military personnel, they would be likely to perceive the differences amongst each other to be less than those between themselves and those US members. As a result, a more inclusive self-category is likely to become salient, say 'ADF personnel' or 'Australians'. Thus, as alluded to in the previous discussion of social identities, the self-categorization that is likely to become salient at any given time will depend on the nature of the *social comparative* context (Oakes et al., 1994; Turner et al., 1987).

There is however, a second type of 'fit' that determines the extent to which a self-category become salient, so-called 'normative fit' (Oakes et al., 1994). Normative fit is the extent to which the perceived differences between categories are consistent with the perceiver's actual expectations. Self-categorization theory holds that a self-category becomes salient to the extent that people behave in ways that are consistent with the perceiver's expectation *vis-à-vis* the normative content of these categories. So, for example, in the meeting between RAAF, RAN, and ARA personnel about who should bear the brunt of cuts to defence spending, self-categorization in terms of one's chosen Service would be unlikely if the officers were perceived as behaving in unexpected ways, say if representatives from each Service insisted that the spending cuts apply to only their Service's projects. Such altruistic behaviour might be more consistent with a self-categorization at the level of 'ADF officer'.

According to self-categorization theory, a salient self-category leads to a process of *depersonalization* (Turner, 1985; Turner et al., 1987). Depersonalization refers to the 'subjective stereotyping' of the self. More specifically, it is defined as the process whereby an individual comes to perceive themselves as *categorically interchangeable* with other ingroup members. As suggested by Turner (1999):

> At certain times the subjective self is defined and experienced as identical, equivalent, similar to, or interchangeable with a social class of people in contrast to some other class. Psychologically, the social collectivity becomes self. (p.12)

Therefore, depersonalization involves a "cognitive re-definition of the self" (Turner et al., 1987, p. 528; see also Turner et al., 1994) from an individual with unique attributes and traits ("me") to a group member who behaves in accordance with ingroup norms and shares the goals and values of other ingroup members ("we"). According to self-categorization theory, it is the process of depersonalization that underpins group behaviour (Turner et al., 1987; Turner & Haslam, 2001). That is, the shift in self-categorization from the "me" to the "we" not only characterizes group behaviour but makes group behaviour possible (Brown & Turner, 1981).

Summary

To this point, we have reviewed some of the fundamental principles of the social identity perspective and in doing so, have outlined ideas that are central to both social identity theory (Tajfel & Turner, 1979) and self-categorization theory (Turner, 1985; Turner et al., 1987). Central to the perspective as a whole is the idea that people perceive and respond to the world differently when they view themselves as group members rather than as individuals (Turner, 1999; Turner & Haslam, 2001). Core to social identity theory is the social identity concept, that is, the idea that people's sense of self derives in part from their membership of social groups and categories. According to social identity theory, people have an inherent need for a positive evaluation of their social identities and that this involves a process of social comparison from which one's ingroup must remain positively distinct from relevant outgroups. Central to self-categorization theory is the idea that social identities are self-categorizations that may vary in their level of abstraction or 'inclusiveness'. According to self-categorization theory, it is when a self-category at a social rather than a personal level becomes salient that group-level behaviour (i.e., behaving in terms of "we" rather than "me") becomes possible. With these ideas in mind, the balance of the chapter outlines two general hypotheses on how the social identity perspective might account for non-disclosure of classified information members of the ADF.

Two hypotheses of problematic non-disclosure

Preserving positive distinctiveness

According to the social identity perspective, establishing or maintaining a positive social identity is dependent on one's ingroup remaining *positively distinct* from relevant outgroups. Clearly, one can attempt to achieve positive ingroup distinctiveness using a range of strategies. For example, one could accentuate their attitudes associated with (or perceptions of) ingroup superiority (i.e., intergroup differentiation) or favour their ingroup *behaviourally* (i.e., intergroup discrimination) through the allocation of resources, as was the case in the minimal group studies (e.g., Tajfel et al., 1971). Of course, information is also a resource. Indeed, in military and defence contexts, information is arguably one of the most precious of all resources. Following this idea, it would seem pertinent to ask: does non-disclosure of information reflect the establishment or preservation of a valued social identity?

In recent years, some progress in this direction has been made by those working from a social identity framework, albeit in the context of research on organizational communication (Haslam, 2004; Lea, Spears, & Rogers, 2003; Postmes, 2001; Suzuki, 1998; Wigboldus, Spears, & Semin, 1999). Communication is generally understood to involve the transfer of information and its meaning from one entity to another (Katz & Kahn, 1966). Obviously, disclosing classified information constitutes an act of organizational communication since it involves the transfer of a particular class of information and presumably its meaning from one organizational entity to another. Yet, it is important to remember that disclosure is a particular *type* of communication. All disclosures may be communicative, but not all acts of communication are disclosures since they do not necessarily involve the transfer of information that is hidden or concealed. In the context of proposing an answer to the question asked in the preceding paragraph however, accepting disclosure as a particular type of communication would seem warranted.

In terms of those working *explicitly* from a social identity framework, the work of Suzuki (1998) may come closest to demonstrating that non-disclosure may serve what might be termed an 'identity-preserving' function. Suzuki sought to

investigate how the social distance associated with different national identities affected communication patterns in organizations, in this case, large multinationals employing predominantly Japanese and Anglo-North American workers. The assumption here was that workers in such organizations would likely derive a positive social identity along the lines of nationality, that is, they would see those of the same nationality as ingroup members and those of the alternative nationality as outgroup members. Suzuki hypothesized that the maintenance of social identity would manifest in terms of the social distance implicated in employee's communication patterns. Therefore, communication with outgroup members was expected to consist largely of task-specific information, that is, information related to work matters (high social distance) while communication with ingroup members was expected to extend beyond the task-specific to include matters not related to work (low social distance). To test this hypothesis, personnel were asked two key questions: (i) who they communicated with in their organization, and (ii) the type of information they communicated. Findings were generally consistent with expectations. Personnel had more task-specific and less non-task specific communication with outgroup members compared to ingroup members and this pattern was more pronounced amongst those who identified strongly with their national category.

While these results suggest that the maintenance of a valued social identity may manifest as non-disclosure behaviour, evidence that non-*disclosure* (rather than non-communication more generally) may serve identity-related concerns can be garnered if we step outside of the formal social identity literature, and indeed, outside the psychological literature altogether. What is relevant here is the sociological and anthropological work that has examined groups in which non-disclosure of certain information is inextricably linked to group identity, or in other words, groups in which a hallmark of belonging is that certain things can or must be left unsaid. Of course, the exemplar of such groups is the so-called 'secret society'. Simmel (1906) for example, recalls a secret order in the Molucca Islands in which group belonging meant that one must never discuss their initiation experiences at any time. Indeed, in this order, after initiation the candidate was required to not speak at all for a period of weeks, not even to family members (see also Bellman, 1981; Mackenzie, 1967; Tefft, 1980). In conceiving of secret societies more generally however, Simmel (1906) argues the first internal relation amongst members is of "reciprocal confidence" (p.

470) *vis-à-vis* the ability to remain silent about certain issues, often the society's very existence. According to Simmel, there resides in this reciprocal confidence "as high moral value as in the companion fact that this confidence is justified" (p. 473). The association between non-disclosure behaviour and the preservation of a valued identity is also evident in sociological analyses of privacy (Kelvin, 1973; Schwartz, 1968; see also Laufer & Wolfe, 1977). According to Schwartz (1968), the non-disclosure associated with privacy serves a "group preserving function" (p. 741) in that it allows a kind of 'time out' to take place amongst group members. Schwartz also argues that the non-disclosure associated with privacy assists in maintaining status divisions between individual and groups, an issue taken up in earlier research by Goffman (1958).

Later work can be drawn upon to illustrate the idea that non-disclosure may serve to promote or preserve one's group identity. Indeed, some of this work refers directly to the non-disclosure of classified military information in this regard. Kaiser (1980) for instance, conducted a review of the US intelligence community, drawing particular attention to the internal norms and mores that were critical to the community's sense of solidarity and "communal identity" (p. 279). According to this author, the most critical norm in this respect was one of 'internal security', that is, non-disclosure of classified information relevant to the communities activities to perceived outsiders. Indeed, Kaiser argued "[t]he fact that illicit activities within the intelligence agencies went unexposed for decades testified to the importance of this norm" (p. 277). The theme that the norms of the military/defence organizations support non-disclosure over disclosure of certain types of information is also evident in those enquiries made by the US government in the aftermath of September 11, 2001. For example, when questioned as to why the FBI failed to develop a strategy for sharing information with State and local police, its Deputy Assistant Director for Counterterrorism replied "[t]he culture says you don't share that information" (House Permanent Select Committee, 2002, p. 358).

At this point, we are left with a general hypothesis regarding the psychology of problematic non-disclosure as it might apply to classified information in the ADF context. Drawn largely from work conducted within the tradition of social identity theory (Tajfel & Turner, 1979) and supported by research that has been conducted

both within and outside of the broader social identity tradition we can hypothesise that non-disclosure of classified information, particularly that which may surface around Service boundaries, reflects the desire to establish and/or maintain positive Service distinctiveness and thereby positive Service identity. However, based on the theoretical review of the social identity perspective above, an alternative hypothesis can also be devised, one in which the self-category that is salient at the time of one's disclosure decision (i.e., the perceived ingroup/outgroup memberships) is central.

A self-categorical gulf

According to the social identity perspective, one's social identities are to be understood as *self-categorizations*, that is, categorizations of the self as being similar and equivalent to other ingroup members, and different from outgroup members (Onorato & Turner, 2002, 2001; Turner et al., 1987; Turner & Onorato, 1999). As outlined earlier, self-categorization theory holds that when a particular self-category becomes salient, a process of depersonalization occurs whereby the self becomes categorically interchangeable with other ingroup members. It is this process that transforms "my" interests into "our" interests and in so doing underpins all collective behaviour.

Following this idea, it would seem pertinent to ask: do patterns of non-disclosure reflect the ingroup/outgroup memberships that are salient at a particular time? In other words, does non-disclosure signify a self-categorical gulf amongst the ADF's army, navy and air force personnel? To date, social identity theorists interested in the effects of manipulating one's perceived ingroup/outgroup memberships (i.e., the salient self-category) have not adopted disclosure behaviour as one of their primary dependent variables. However, their interest has focused on other, more general outcome variables of which disclosure behaviour can be seen to represent. As mentioned in Chapter 3, one of these is *cooperation* and a second is the concept of *trust*.

Social identity processes & cooperation

Generally speaking, cooperation refers to instances where people work together to accomplish shared tasks and one's behaviour is 'cooperative' to the extent

that it intends to benefit the group rather than the individual (Boyd & Richardson, 1991; Tyler, 1999; Tyler & Blader, 2001). In recent years, researchers working from a social identity framework have investigated more fully the nature of the psychological processes underlying an individual's decision to engage in cooperative behaviour at work (e.g., Ellemers, Van Rijswilk, Bruins, & de Gilder, 1998; Tyler, 1999, 2001; Tyler & Blader, 2000, 2001). The basic idea here is that the extent to which an individual identifies with an organization (or a particular organizational group) is positively associated with the willingness of workers to behave cooperatively toward the organization (or organizational group) by complying with its rules, helping other members, and remaining a member (Tyler, 1999; Tyler & Blader, 2000, 2001).

This core idea can be traced back to earlier studies in the social identity tradition which demonstrated that people are relatively more willing to cooperate in an organizational context when they perceive the organization and it members to be a positively valued ingroup rather than a negatively valued outgroup. Brown (1978) for example, examined the relations between the production and development sections of a large British factory. In this study, 41 shop stewards representing the two sections were interviewed and asked how they would respond to a threat where the factory workforce *as a whole* faced large-scale redundancies. Results showed that 80% of interviewees did not spontaneously suggest a course of action that involved cooperation between the sections and/or their unions representatives. Brown (1978) argued that this reflected a history of often hostile social comparison and intergroup differentiation between the two sections which had intensified in the context of a recent wage restructuring proposal. In other words, the lack of cooperation was seen to stem from a lack of a positively-valued superordinate identity.

More recently, Ellemers, Van Rijswilk et al., (1998) examined the link between social identification processes and cooperation in a study of power use in a simulated organization. These researchers reasoned that the willingness of workers to cooperate with superiors who exercised excessive power would vary according to whether the superior was perceived as an ingroup or outgroup member. To test this idea, study participants were asked to perform a stock-trading task whereby they made decisions about buying or selling stocks under the supervision of a superior who was

either an ingroup or outgroup member and who wielded either high or low power (via the number of decisions that they overruled). Results showed that participants were equally willing to work cooperatively with an ingroup superior regardless of the amount of power they exercised, but were less willing to cooperate with an outgroup superior who had exercised high power. More importantly perhaps, participants were more willing to work cooperatively as their identification with (i.e., commitment to) their superiors increased. Ellemers, Van Rijswilk et al., (1998) concluded that identification with a superior can promote interpersonal cooperation even when the superior's leadership style is evaluated poorly (see also Bruins, Ellemers, & de Gilder, 1999).

Studies conducted from a social dilemmas framework also demonstrate how a salient social identity is able to transform individualistic behaviour into cooperative behaviour. Social dilemmas can be defined as situations where an individual faces a choice about whether to act in terms of their own personal interest (i.e., "defecting") or in the interests of a group to which they belong (i.e., "cooperating"; see Komorita & Parks, 1996). More formally, social dilemmas have an interdependence structure in which defecting yields a higher payoff for oneself than does cooperating regardless of what other group members do, yet if everyone defects, all will receive a payoff that is less preferable than that which would have obtained if all cooperated (Smithson & Foddy, 1999). It has been widely hypothesized that people are willing to make cooperative decisions in social dilemmas to the extent to which they perceive the others involved to be ingroup members.

Wit and Wilke (1992) for instance, organized study participants into 10 person teams, presenting each member a particular kind of social dilemma in a real-world format (e.g., a traffic-congestion problem)[9]. Participants were told that their payoffs would manifest as tokens that could be spent on refreshments later, but that due to a shortage of tokens a certain allocation procedure would have to be followed. In the group categorization condition, participants were told that only members of randomly selected groups would receive their tokens. In the personal categorization condition,

---

8. Wit and Wilke (1992) employed the Chicken Dilemma Game (CDG), Trust Dilemma Game (TDG) and Prisoner's Dilemma Game (PDG).

participants were told that only randomly selected individuals would receive their tokens. The findings showed that this manipulation had a number of significant effects. As expected, participants in the group categorization condition were more cooperative in their dilemmas choices than those in the personal categorization condition. Further, those in the group categorization condition *expected* more cooperation from their group colleagues, than did those in the personal categorization condition. Additionally however, they also believed that their group was more cooperative compared to other groups participating in the study, than did those in personal categorization condition. In other words, group categorization resulted in a positive differentiation of the ingroup from other groups in terms of the perceived cooperativeness of ingroup members (see also De Cremer & Van Vugt, 1999; Orbell, Dawes, & Schwartz-Shea, 1994).

Social identity processes & trust

In Chapter 3, we argued that disclosure outcomes are likely to be reflected in the extent to which the potential discloser of the information trusts its potential recipient. The idea that trust underpins important organizational processes is also a major theme in the broader organizational literature. Here, there is an almost universally held assumption that organizational success is positively associated with *and possibly determined by* the extent to which members trust each other (e.g., Jones & George, 1998; Kramer, 1999, 2001; Lewicki & Bunker, 1995; McAllister, 1995; McCauley & Kuhnert, 1992). This assumption is based on the results of studies which have shown that trust has a positive influence on many important organizational outcomes including cooperation (Costigan, Ilter, & Berman, 1998; Hagen & Choe, 1998; Jones & George, 1998; Lane & Bachman, 1996; Madhok, 1995), communication (Chandra-Sekhar & Anjaiah, 1995; Roberts & O'Reilly, 1974), problem solving (Zand, 1972), and profit (Davis, Schoorman, Mayer, & Hoon Tan, 2000). Not surprisingly then, increasing attention has been focused on the antecedents of organizational trust (Adams, Bryant, & Webb, 2001; Kramer, 1999).

The antecedents of organizational trust pose an interesting problem for trust theorists and researchers. Traditionally, trust is thought to stem from a process of repeated and incremental interaction between the trustee and the trustor, allowing the

former *to become known* to the latter (see Boon & Holmes, 1991; Deutsch, 1958). However, the complexity of modern organizational structures and environments, and the increasing trend toward 'temporary' organizational structures, is seen to restrict the extent to which an individual member can build up 'evidence-based' knowledge about the trustworthiness of other members (Kramer, 2001, 1999; Kramer, Brewer, & Hanna, 1996; Meyerson, Weick, & Kramer, 1996). Military organizations are no exception in this respect with posting cycles that tend to last around three years and a trend toward the "rapid" formation and deployment of military Headquarters with a lifespan limited to the duration of a particular conflict or crisis (see Adams et al., 2001; Dorman et al., 1998). Given then, that reputation-building may be problematic in organizational contexts, factors other than personal interaction history have been considered as antecedents of trust. One of the most influential ideas to emerge in this regard is that people use information about the social categories to which others belong (e.g., police officers, used-car salesmen, clergy, and so on) to inform and shape their trust-related decisions (Brewer, 1981; Williams, 2001). This idea provides a backdrop to the view that trust is an outcome of social identity processes and the concepts of 'depersonalized trust' (Brewer, 1981), 'category-based trust' (Kramer, 1999) and 'identification-based' trust (Kramer, 2001; Kramer et al., 1996; Lewicki & Bunker, 1995) are all used somewhat interchangeably in this regard. For those working from a social identity perspective, a salient social identity is thought to provide a *presumptive* basis for the placement of trust in others (Brewer, 1981; Kramer, 2001; Kramer et al., 1996). More specifically, when an individual shifts from a personal to a social level of identity, trust is able to be conferred on other ingroup members solely on the basis of their shared category membership (Kramer, 1999). As Brewer (1981) argues:

> Common membership in a salient social category can serve as a rule for defining the boundaries of low-risk interpersonal trust that bypasses the need for personal knowledge and the costs of negotiating reciprocity...Within categories the probability of reciprocity is presumed, a priori, to be high, while between categories it is presumed to be low or subject to individual negotiation (p. 356).

Supporting this idea is the frequent finding that people perceive ingroup members to be more trustworthy than outgroup members (Allen & Wilder, 1975; Brewer, 1979; Brewer & Silver, 1978; see also Messick & Mackie, 1989). A number

of cognitive-motivational mechanisms and models have been advanced surrounding this association emphasizing either the perceived similarity of ingroup members (Brewer, 1981), group norms as a means to protect against trust violations (Brewer, 1981; Greenberger et al., 1987), the benefits of displays of trust (Kramer, 2001; Fine & Holyfield, 1996), or the role of affective processes (McAllister, 1995; Williams, 2001). However, the fundamental process according to the social identity perspective is depersonalization (Turner, 1985; Turner et al., 1987). When one perceives themselves to be categorically interchangeable with other ingroup members (i.e., when a self-category at a social level becomes salient), psychological distance between group members decreases, and people becomes oriented toward their shared or joints goals and away from their individual goals, promoting both the placement and fulfilment of trust.

Given that self-categorization processes are dynamic and that self-category salience is determined (in part) by the nature of the prevailing social context (Turner et al., 1987), the extent to which trust is present can be expected to change with the social context. For example, trust between Air Force and Navy personnel may be heightened when an inclusive self-category (i.e., ADF) is salient, say in the context of planning a high-profile Air-Sea rescue operation. Yet, if the salience of this inclusive self-category were to disintegrate, say if the operation was a major failure and each Service blamed the other, levels of inter-Service trust would likely fall. Further, the extent to which trust is present can be expected to change according to whether the dimension on which it is potentially placed is relevant to the salient ingroup identity. Just because Navy personnel trust their Air Force counterparts to provide them with accurate surveillance information does not mean they also trust their knowledge about the best ways to support naval elements with air power.

Chattopadhyay and George (2001) recently sought to investigate the social identity processes underpinning intergroup trust in an organizational context. Drawing on the idea that employees often form social identities around their work status, that is, whether they are employed on a permanent or temporary basis these researchers hypothesised that work status dissimilarity would constitute a salient ingroup-outgroup boundary that could be expected to have a negative impact on intergroup trust. To test this idea, they surveyed employees from two large computer

manufacturing organizations. Results showed that in contexts where work status dissimilarity was particularly salient, in this case, when permanent employees were numerically outnumbered by their temporary counterparts, members of the former (high status) group attributed lower levels of trust to members of the latter (low-status) group (see also Chattopadhyay, 1999; Veenstra, 2003).

Again, we are left with a second hypothesis regarding the psychology of problematic non-disclosure as it might apply to classified information in the ADF context. This hypothesis is drawn largely from work conducted within the tradition of self-categorization theory (Turner, 1985; Turner et al., 1987) and supported by research within this tradition concerning the psychology of cooperation and trust. Specifically, we could hypothesise that non-disclosure of classified information, particularly as it may relate to Service boundaries, reflects the particular self-category (i.e., the perceived ingroup/outgroup memberships) salient at the given time.

Summary and conclusion

In this chapter, the main principles of the social identity perspective as they apply to the psychological basis of ingroup favouritism have been reviewed, as have the contributions of the social identity perspective towards understanding trust, cooperation, and communication in intergroup settings. A number of important points emerge from this analysis. Primary amongst them is the idea when an individual's membership of a particular social group makes a positive contribution to how they view themselves, they will seek to positively differentiate this group from other groups in the social context. As has been shown in the applied literature reviewed above, positive differentiation may manifest in various ways, including one's perceptions about the trustworthiness of others and the extent to which they are willing to cooperate or communicate with them. This analysis suggests that the Service-loyal disclosure of classified information in the ADF may be related to the extent to which ADF personnel seek to positively differentiate their Service vis-à-vis each other. Also of particular significance is the idea that organizational outcomes will be determined, to some extent, by the particular level at which people categorise themselves (Haslam, 2004). This implies, that any Service-loyal disclosure gradient could be transformed into one more consistent with the ideology and doctrines of

Jointness through the establishment of salient self-category that crosses inter-Service boundaries. These ideas are explored empirically in the next chapter.

CHAPTER 6

TESTING THE TWO HYPOTHESES:

JOINTNESS AND THE SELF-CATEGORICAL GULF

Introduction

In Study 1, we sought to determine if, when, and for whom ADF personnel would breach official rules in order to avert problematic non-disclosure. Amongst other things, our findings suggested a role for the potential discloser's group (in this case, Service) affiliation. Specifically, we found that ADF personnel tended to be more willing to disclose the information to the unofficial request when doing so would prevent harm befalling their own Service compared to when the harm would befall another Service. This suggestion that problematic non-disclosure of classified information in the ADF is likely to surface around Service boundaries pointed the way toward bringing some theoretical rigour to the problem. To that end, in the previous chapter we reviewed the social identity perspective, a theoretical framework that encompasses social identity theory (Tajfel & Turner, 1979) and self-categorization theory (Turner, 1985, Turner et al., 1987) and examines how perceptions of and responses to the social and organizational world are qualitatively different when people see themselves as group members rather than as individuals.

From this review, two general hypotheses of non-disclosure of classified information in the ADF emerged. The first holds that non-disclosure is a form of ingroup favouritism driven by the need to establish, maintain or protect Service distinctiveness and thereby Service identity. According to this hypothesis, the degree of problematic non-disclosure around the ADF's Service boundaries could be expected to vary to the extent that positive Service distinctiveness is threatened. The second hypothesis holds that, rather than being driven by a perceived or actual threat to Service distinctiveness, non-disclosure of classified information (like cooperation more generally) follows the contours of the ingroup/outgroup memberships that are salient for the potential discloser at that particular time. Here, the degree of problematic non-disclosure likely to surface around Service boundaries could be

expected to vary to the extent that these boundaries represent the salient level of self-categorization for the potential discloser at the time of their decision-making.

The aim of this chapter is to test these hypotheses. However, and as mentioned above, we now move away from addressing the psychology of problematic non-disclosure directly (i.e., explicitly) as was the case in the pilot study and Study 1. We also move away from issues associated with the potential breach of official rules. Instead, our approach in this chapter (and for the remainder of the thesis) is to focus on "routine" circumstances involving the potential disclosure of classified information, specifically, those in which the potential discloser is requested for classified information from a potential recipient. This is an "indirect" approach in the sense that we seek to gain insight into the factors implicated in problematic non-disclosure of classified information by examining ADF personnels' perceptions of, and responses to, routine requests for its disclosure. Of course, such responses can manifest in many ways other than an outright decision to disclose or not disclose. These may include delaying a decision, seeking advice, verifying the potential recipient's credentials beyond what is necessary, or passing responsibility for the disclosure decision to someone else entirely. Our approach from this point on also focuses on the *content* of the information likely to be central to problematic non-disclosure. As suggested in the previous chapter, problematic non-disclosure appears particularly likely to involve information about one's group that is sensitive to its overall interests (Kaiser, 1980). Hence, our focus has tightened somewhat to consider the potential disclosure of information that is not only classified but 'Service-sensitive' in some way. Therefore, we could expect the potential discloser's perceptions about the trustworthiness of the potential recipient to become more important in shaping disclosure outcomes.

To that end, two studies are presented in this chapter. The first hypothesis outlined above is tested in Study 2 where it is 'situated' within a manipulation of the Jointness ideology. For some time, a constant theme within discussions of Jointness has been the potential for the ideology to threaten Service distinctiveness (Codner, 1998; Fautua, 2000; Trainor, 1993-4). In essence then, Study 2 asks whether Jointness constitutes a vehicle by which Service distinctiveness is undermined and if so, whether it is likely to be part of a problem *vis-à-vis* problematic non-disclosure of

classified information in the ADF. Of course, if Jointness turns out to be part of any such problem, the principles embedded within this hypothesis help specify how it may also be part of the solution.

The second hypothesis is tested in Study 3 where it is situated within a manipulation of a 'shared opinion group' (see McGarty & Bliuc, 2004). Set against the backdrop of social identity research into the effects of 'recategorization' (e.g., Dovidio et al., 1997), we ask in Study 3 whether disclosure of classified information is a function of the salient level of self-categorization, that is, if it follows the perceived ingroup-outgroup memberships salient at the time of decision-making. If so, it follows that the disclosure of classified information could be 're-routed' by changing these perceived memberships.

Study 2

Introduction

As discussed in Chapter 5, an idea central to the social identity perspective is that people seek to positively differentiate their ingroups from comparable outgroups (Tajfel & Turner, 1979; see also Turner & Reynolds, 2001). In other words, in order to make a positive contribution to social identity, a group must remain *positively distinct* from other groups in the comparative context (Tajfel, 1978). It follows from this idea that a superordinate categorization or ideology that downplays or indeed eliminates intergroup boundaries, either purposefully or inadvertently, impedes the ability of the included groups to positively differentiate themselves from one another (Hornsey & Hogg, 2000a). In short, such categorizations and ideologies may be seen by group members to be undermining group distinctiveness (Hornsey & Hogg, 1999, 2000a, 2000b; van Leeuwen & van Knippenberg, 2003).

In the social identity literature, categorizations and ideologies that undermine group distinctiveness are viewed as 'threats' to social identity (Branscombe, Ellemers, Spears, & Doosje, 1999; Jetten et al., 1999). Further, research shows that such threats frequently evoke an intensification of ingroup favouritism in an effort to restore the group's positive distinctiveness (Hornsey & Hogg, 1999, 2000a; Jetten et al., 1999;

Mlicki & Ellemers, 1996; Roccas & Schwartz, 1993; van Leeuwen, van Knippenberg & Ellemers, 2001). For instance, Hornsey and Hogg (2000b) argue that distinctiveness threats often result in group members asserting their group identity, sharpening their perception of intergroup boundaries, and accentuating their sense of ingroup solidarity. Research in the tradition has also shown that the extent to which threats to social identity evoke ingroup favouritism often varies according to one's level of identification with the threatened group (Jetten et al., 1999). Not surprisingly, those who identify strongly with the threatened group (so-called "high-identifiers") usually display the greatest ingroup favouritism in response to identity threats while those who identify only marginally with threatened group (so-called "low identifiers") however, generally respond with ingroup favouritism to a lesser degree, or may even welcome the categorization or ideology that undermines group distinctiveness (e.g., Spears, Doosje, & Ellemers, 1997). According to self-categorization theory (Turner, 1985; Turner et al., 1987) the extent to which an individual identifies with a given social group or category reflects the extent to which that particular self-category is central and of evaluative importance to one's self-definition, and is thus related to the notion of perceiver readiness (Turner, 1985; Turner et al., 1987).

On the basis of these ideas, there has emerged a general consensus amongst social identity theorists that cooperative intergroup relations are likely to depend on superordinate categorizations and ideologies that *preserve* rather than eliminate subgroup distinctiveness (Hornsey & Hogg, 2000b; see van Leeuwen & van Knippenberg, 2003)[10]. Indeed, this message has become central to many models of intergroup relations including the recategorization model proposed by Gaertner et al., (2000), the Mutual Intergroup Differentiation Model (Hewstone & Brown, 1996), the ASPIRe model (Haslam et al., 2003), and Optimal Distinctiveness Theory (Brewer, 1991). This idea also resonates within Western military organizations including the ADF, primarily in relation to the concept of Jointness. Since Jointness was formally conceived after the end of World War II, it has remained a source of considerable tension amongst military personnel primarily because of its perceived potential to undermine the distinctiveness of the individual Services (Trainor, 1993-4; see also Dunn, 1995, Fautua, 2000). As the number of recent publications on this issue would

9. This reflects the debate in the broader cultural relations literature between the benefits of multiculturalism over assimilationist policies (see Berry, 1976; Hornsey & Hogg, 2000a, 2000b).

suggest, this tension shows little sign of abating (see Ankersen, 1998; Codner, 1998; Fautua, 2000; Owens, 1993-94; Sapolsky, 1997; Wilkerson, 1997). Alluding to the social identification processes described above, Beaumont (1993) provides an eloquent description of the tension:

> Armies, navies, and air forces must be able to restore and regenerate after major destruction and heavy losses. They function in the face of death, maiming, mutilation, capture, and punishment, condition with no counterpart in civil life aside from, and then only briefly major catastrophes...It is not surprising, then, given the hunger for strong, well-demarcated allegiances and identities found among warriors, that many have resisted cooperation, fusion, and jointness. (p. 185)

Our question now is whether problematic non-disclosure of classified information in the ADF is likely to surface around Service boundaries because of a perceived threat to Service distinctiveness that is evoked by Jointness.

To address this, we will present ADF personnel with two antithetical views of Jointness, one advocating the irrelevance and removal of Service distinctiveness, the other advocating its importance and preservation. Along the lines suggested above, we expect that the former will constitute a threat to Service distinctiveness while the latter will not. More importantly however, we expect the former, what we will term "threatening Jointness" to evoke disclosure outcomes that are more Service-loyal than those evoked by the latter or "non-threatening Jointness". As discussed above, the disclosure outcomes here relate to those courses of action which ADF personnel are likely to take in response to a request to disclose classified information that is also sensitive in terms of one's Service interests. We formulate this general hypothesis in the broader context of investigating how the potential discloser's affiliations impact the disclosure of classified information. Yet, and in light of the results of Study 1, we must also accept that a role will be played by risk in this respect. Specifically, we could expect threatening Jointness to lead to Service-loyal disclosure outcomes only when non-disclosure would not risk key ADF goals. Formally, the hypotheses of Study 2 are summarised below:

H1. Threatening Jointness will evoke Service-loyal disclosure outcomes to a greater degree than non-threatening Jointness. This will be moderated by:

(a) Perceived risk to the ADF, in that the Service-loyal disclosure will be confined to circumstances where risk to the ADF is low;

(b) Identification, in that the Service-loyal disclosure will likely be accentuated amongst those who identify strongly with their Service.

Method

Participants and design

Eighty-nine ADF personnel took part in Study 2. This comprised 60 members of the RAN drawn from Navy Headquarters and a nearby RAN establishment and 29 members of the ARA drawn from Army Headquarters. Most were men ($n = 74$) and the mean age was 38 years. Of those commissioned, most were of Major-equivalent rank or above ($n = 45$) with a small number of Captain (Army) equivalent rank or below ($n = 7$). The remaining 35 participants were non-commissioned officers (NCOs). Two participants did not indicate their rank. Participants had served an average of 18 years in the ADF and most ($n = 59$) held a TOP SECRET clearance.

The study had a 2 (Jointness: threat/no-threat to Service identity) x 2 (risk to ADF: low/high) x 2 (requester's Service: own/other) mixed within-between participants design. The first two independent variables were manipulated between-participants while the third was manipulated within-participants.

Participants were given a questionnaire in which they were told that a stated opinion and a short scenario provided the backdrop to a number of questions. The stated opinion was one about Jointness in the ADF and advocated either the irrelevance and removal of Service distinctiveness ('threatening Jointness') or the importance and preservation of Service distinctiveness ('non-threatening Jointness'). Immediately following their responses to the stated opinion, participants were given a

short scenario in which they were asked to imagine receiving a request for a certain piece of classified information from another member of the ADF. Following this, they were asked to respond to a number of questions assessing their perception of the requester (i.e., potential recipient) and their likely response to the request.

Materials and procedure

Four versions of the study questionnaire were developed, one corresponding to each of the between-subjects conditions (see Appendix B). Each questionnaire was copied on DSTO letterhead and attached to a covering letter that invited participation in a research program examining the "knowledge environment" of the ADF. The covering letter also stated that participation was voluntary and that all information collected would remain anonymous. Questionnaires were randomly distributed to ADF personnel in the participating organizations, facilitated by the respective Chief of Staff or Commanding Officer.

Manipulation of Jointness (Service identity threat)

Upon opening the questionnaire, participants were instructed to read "one of the most common opinions" held by members of the ADF about Jointness. In the 'threatening Jointness' condition, the opinion read as follows:

> In the ADF, we work as a Joint team - a team where Jointness sets the standards, a team that knows Jointness is inseparable from real capability...
>
> The single-Service ethos is dead (or it should be dead). Retaining a 'single-Service mentality' is an excuse for not moving with the times. Ridding ourselves of single-Service traditions and replacing them with Joint values is the way to achieve responsiveness.
>
> In Jointness, the potential of our forces is realised. Outdated ideas about 'single-Service loyalty' compromise that potential. Such loyalty has no relevance, as our future is Joint.

In the 'non-threatening Jointness' condition, the stated opinion read as follows:

> In the ADF we must work as a Joint team - one capable of integrating the unique abilities of each Service, one that can focus single-Service strengths into optimal capabilities.
>
> Our single-Service traditions are the building blocks of Jointness. They are, after all, highly relevant to Service ethos and performance. Complementing strong Service traditions and ethos with Joint concepts, where appropriate, is the way to achieve responsiveness.
>
> Jointness should not get in the way of the Services - it should help each Service to achieve the best overall outcomes.

In both conditions, the opinion was fabricated by the experimenter (working in consultation with serving and former ADF officers). Participants then responded to a series of questions on 7-point Likert-type scales.

Following this, participants were instructed to imagine the following scenario (bracketed terms indicate wording used to match questionnaires to participant's Service):

> You work in an [Army/Navy] Headquarters. As part of your usual work duties, you receive information about the readiness of certain force elements belonging to the [Army/Navy].
>
> On this occasion, you are one of several [Army/Navy] personnel privy to classified information that details a temporary lack of readiness of some force elements. The reasons for this lack of readiness would be clear to [Army/Navy] personnel, however this information could be interpreted by other personnel in a way that would severely damage the image of the [Army/Navy].

Manipulation of risk to ADF

In the low risk to ADF condition, the scenario concluded with the following:

> Elsewhere, a Joint area is preparing a report on how the principles of Jointness can be used to improve the readiness of force elements.

In the high risk to ADF condition, the scenario concluded with the following:

> Elsewhere, a Joint area is preparing plans for an imminent Joint operational deployment which may require those affected force elements.

Manipulation of the requester's Service

After reading the end of scenario, participants were asked to imagine that they received a request for the potentially damaging information from a member of the said "Joint area" who held an adequate security clearance and who was from either their own Service or another Service. As the latter was manipulated within-participants, the ordering of the requester's Service was counterbalanced across conditions (i.e., an own-Service requester then an other-Service requester, or vice versa). Participants then responded to a series of questions on 7-point Likert-type scales.

Dependent measures

At the very beginning of the questionnaire, participants responded to three items measuring the extent to which they identified with their Service: (1) "I identify with my Service", (2) "I feel strong ties with the personnel of my Service", and (3) "I am committed to the aims of my Service".

Following the manipulation of Jointness, participants rated the extent to which they agreed with five statements. The first three measured the extent to which they endorsed the view of Jointness presented: (1) "I share this view of Jointness"; (2) "This view of Jointness should be widely accepted by all members of the ADF", and (3) "This view of Jointness is compatible with the traditions of my Service". The remaining two items measured the extent to which they believed that the view of Jointness presented was being promoted in the ADF context: (4) "This view of Jointness has been imported into the ADF from other military organizations (e.g., in

Canada, U.S.)"; (5) "This view of Jointness is being pushed by some prominent parts of the ADF". Collectively, these items served to check the manipulation of Service distinctiveness threat, where relatively low scores on items (1) - (3) (i.e., non-endorsement) coupled with high scores on items (4) and (5) (i.e., perceived pressure to endorse) were assumed to reflect a state of ideological threat (Kenworthy, in press).

To check the manipulation of perceived risk to the ADF, participants were asked the following: "If this information is not provided to anyone in the Joint area, how likely do you think it is that key ADF objectives will be compromised?".

Following the disclosure scenario, participants were asked to respond to six questions relating to their perception of, and likely response to the requester. The first question assessed the extent to which participants trusted the requester in this context: (1) "To what extent would you trust this individual not to allow the information to damage the image of the [RAN/ARA?]" (*trust*). The remaining items assessed the extent to which participants would be likely to take various courses of action in response to the request. Specifically, they were asked how likely they would be to:

(2) "Provide the information to the requester without further consultation?" (*disclose*);
(3) "Delay responding to the request in anticipation of a change in readiness?" (*delay*);
(3) "Personally verify the requester's clearance and/or 'need-to-know'?" (*verify*);
(4) "Seek advice from Service peers before deciding whether to disclose?" (*seek*);
(5) "Pass the responsibility for dealing with the request up the chain of command?" (*pass*).

These questions were then repeated for the own/other-Service requester. Responses to all dependent measures were recorded on 7-point scales with end-points "Not at all" (1) and "Very likely" (7) or the relevant equivalents.

Finally, demographic information including age, sex, rank, length of ADF tenure, and level of security clearance was collected. Participants were thanked for their time and invited to provide comments.

Results

Missing data

There were thirteen cases of missing data. In each case, the median score on the item for the sample as a whole was substituted.

Data reduction

As there was a high degree of inter-item reliability between the three items used to measure participants; identification with their Service, they were collapsed to create a single scale ($\alpha = .86$). A high degree of inter-item reliability was also evident between the three items measuring the extent to which participants endorsed the view of Jointness presented. Hence, these were collapsed to create a single 'Jointness endorsement' scale ($\alpha = .90$).

Manipulation checks

With respect to the manipulation of Jointness (i.e., Service identity threat) means on the Jointness endorsement scale differed significantly across the threatening/non-threatening Jointness conditions in the expected direction (*M*s=3.38, 5.08, $p<.001$). However, inspection of frequency histograms showed that in the threatening Jointness condition, the distribution of responses on this scale was markedly bimodal (see Figure 6.1). In other words, a sizeable proportion of participants expressed a degree of non-endorsement of threatening Jointness and a comparable proportion a degree of endorsement for this view. Means on the item assessing the extent to which the view of Jointness presented was seen to be "imported" into the ADF from overseas did not differ across the threatening/non-threatening Jointness conditions (*M*s=4.23, 4.12, respectively), nor did those on the item assessing the extent to which it was seen to be being "pushed" by prominent parts of the ADF (*M*s=4.81, 4.71, respectively). Therefore, our manipulation of Service distinctiveness threat was only marginally successful.

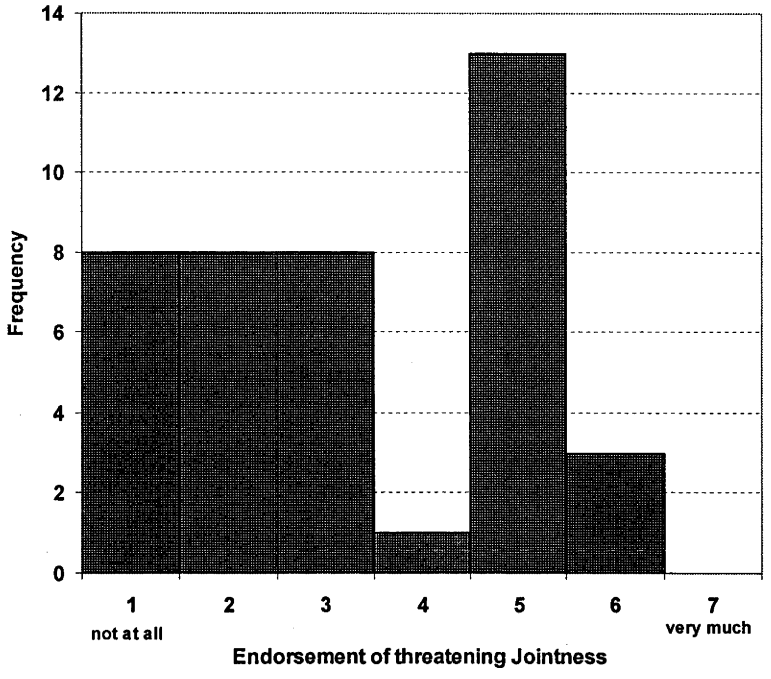


Figure 6.1 Frequency responses to threatening Jointness.

Confirming the success of the risk to ADF manipulation, non-disclosure was seen to present a greater risk to key ADF goals when the information was required for an imminent operation ($M = 5.17$) than for a report on how Jointness could improve force readiness ($M = 4.36$; $t(84) = 2.34$, $p<.05$). However, it should be noted that both means are moderate and thus provide a somewhat weaker manipulation of high and low risk than was desired.

Analysis of variance (ANOVA)

Means and standard deviations for the key dependent measures (courses of action) are shown in Table 6.1.

Table 6.1

Means and standard deviations for courses of action as a function of Jointness and risk to ADF.

Jointness	Threatening		Non-threatening	
Risk to ADF	High	Low	High	Low
Course of action	Own Service requester			
Trust	4.54 (1.67)	4.75 (1.57)	4.37 (1.80)	4.32 (1.76)
Disclose	3.33 (2.18)	3.21 (1.89)	3.42 (1.71)	2.23 (1.34)
Delay	2.58 (1.84)	2.96 (1.52)	3.21 (2.02)	3.91 (1.95)
Verify	5.75 (1.78)	5.62 (1.44)	5.26 (1.66)	6.05 (1.43)
Seek	5.00 (2.06)	5.58 (1.64)	4.89 (1.82)	5.32 (1.94)
Pass	4.46 (2.30)	4.46 (1.98)	4.11 (2.08)	4.77 (1.72)
	Other Service requester			
Trust	3.75 (1.75)	3.58 (1.61)	3.42 (1.61)	3.18 (1.71)
Disclose	3.04 (2.14)	2.87 (1.73)	2.89 (1.63)	2.18 (1.56)
Delay	3.21 (2.19)	3.29 (1.78)	3.32 (2.14)	4.00 (1.90)
Verify	5.92 (1.67)	6.00 (1.25)	5.32 (1.46)	5.91 (1.60)
Seek	5.17 (2.18)	5.54 (1.77)	4.79 (2.10)	5.27 (2.12)
Pass	4.75 (2.31)	4.96 (1.90)	4.32 (2.24)	5.00 (1.95)

Scores for key dependent measures were submitted to a 2 (requester's Service: own/other) x 2 (Jointness: threatening/non-threatening) x 2 (risk to ADF: low/high) mixed within-between participants ANOVA (see Table 6.2).

Table 6.2

ANOVA statistics for courses of action as a function of Jointness, risk to ADF, and requester's Service.

Source	*df*	*F*	η^2	*p*
	Between participants			
Jointness (J)	1	0.56	.01	.46
Risk (R)	1	1.17	.01	.28
J x R	1	0.15	.00	.70
Subjects within-group error	85	(6.78)		
	Within participants			
Requester's Service (S)	1	3.83	.04	.05*
S x J	1	2.85	.03	.10
S x R	1	0.07	.00	.79
S x J x R	1	0.28	.00	.59
S x Subjects within group error	85	(0.71)		

Note. Values enclosed in parentheses represent mean square errors.
*p = .05;

Results of this analysis revealed a main effect for the requester's Service ($F_{(1,85)} = 3.83, p = .05$) of small effect size. There were no other main effects or interactions, hence we found no support for H1.

In order to more fully investigate the impact of the requester's Service manipulation, scores on key dependent measures were collapsed across between-participants factors and submitted to a 2 (requester's Service: own/other) x 6 (potential courses of action) repeated measures ANOVA. Results indicated no main effect for requester's Service but a significant interaction between requester's Service and the likely course of action ($F_{(1,88)} = 16.96, p < .001; \eta^2 = .16$). Post-hoc analysis revealed that compared to another-Service requester, participants: trusted an own-Service requester more (Ms = 3.49, 4.51, $p < .001$); were more likely to provide the information to own-Service requester without further delay (Ms = 2.75, 3.04, $p < .05$); were less likely to delay responding to an own-Service requester (Ms = 3.45, 3.15, $p < .01$); and were less likely to pass responsibility for dealing with the request from an

own-Service requester up the chain-of-command (*M*s = 4.78, 4.46, $p<.001$). However, the requester's Service had no impact on the likelihood of verifying the requester's security clearance and/or need to know details, or seeking advice from one's Service peers on how the deal with the request.

Correlational analyses were conducted in order to examine any association between the perceived trustworthiness of own- and other-Service requesters and the potential courses of action. Results are presented in Table 6.3.

Table 6.3

Correlations between trust in own- and other-Service requesters and course of action.

	Course of action				
	Provide	Delay	Verify	Seek	Upchain
Trust (own-Service requester)	.54**	-.08	-.10	-.21	-.28**
Trust (other-Service requester)	.50**	-.14	-.41**	-.28**	-.45**

** $p < .01$

For both own and other-Service requesters, trust was positively related to the likelihood of providing the information without delay and negatively related to the likelihood of passing the request up the chain of command. However, for other-Service requesters, trust was also related to the likelihood of verifying security clearance and/or need-to-know details and seeking advice about how to deal with the request.

Discussion

The aim of Study 2 was to test the first of our hypotheses of problematic non-disclosure derived from the social identity perspective. It was hypothesized that the degree of problematic non-disclosure of classified information likely to surface around Service boundaries would vary to the extent to which participants felt that the distinctiveness of their Service was threatened. We reasoned that when the ideology of Jointness is viewed as a threat to Service distinctiveness, as many have recently argued (e.g., Ankersen, 1998; Codner, 1998; Trainor, 1993-4), participants' disclosure

intentions would be more Service-loyal than when Jointness is viewed as preserving or promoting Service distinctiveness. We also expected this pattern to be moderated by the degree of risk to the ADF associated with non-disclosure and the level of participant identification with their Service (H1).

Yet, support for H1 was not forthcoming in that there was no interaction between the requester's Service, the manipulation of Jointness, and risk to the ADF on participants' likely courses of action. Indeed, our manipulation checks suggested that both manipulations obtained less than ideal support. Importantly, these checks indicated that "threatening Jointness" did not appear to constitute a clear threat to Service identity. Those participants who were presented with this view of Jointness could be divided into two comparable groups: those expressing some degree of resistance to the view and those expressing some degree of support for it. Further, findings indicated that our sample of participants did not see threatening Jointness as an ideology that was being imported or "pushed" into the ADF any more than non-threatening Jointness. In the face of these results, it was difficult to conclude that Jointness constitutes a clear threat to Service identity and one might argue that this was confirmed by the lack of any subsequent effects on participants' disclosure intentions. While the manipulation of risk to the ADF (associated with non-disclosure) was successful, we can only generalise our results to a scenario of moderate risk.

There are a number of plausible reasons why threatening Jointness did not constitute a clear threat to Service identity. One straightforward possibility is that threatening Jointness was simply not related to those dimensions of Service identity referred to (see Turner, 1978a). We may, for instance, have been more successful in evoking a Service distinctiveness threat by undermining other dimensions likely to be central in this respect, such as Service roles or unique capabilities rather than Service ethos, traditions, and values. However, given that these ethos, traditions, and values are frequently cited as core elements of military affiliation (see Baker, 1995; Beaumont, 1993), it is hard to accept they are irrelevant or 'secondary' aspects of Service identity. A second and related possibility is that Jointness (in any form) is viewed as a task-specific (i.e., operational) ideology and that identity issues may not have the same potency in this task-oriented environment that they might do in other

settings that are less 'outcome-focused'. A third, and again related possibility may lie in the perceived interdependence of the Services. Specifically, ADF personnel may not have wished to express a lack of endorsement for either view presented because of the belief that doing so would undermine a system upon which organizational success as a whole depends (Behm et al., 2001; Dunn, 1995; Hinge, 1996; see also Hornsey & Hogg, 2000a). The following comment provided by one participant contains elements of these ideas:

> Joint is good for operations and capability. Joint customs and traditions will never work. In most cases, when you say Joint to Navy, that means Army is in charge. (Participant 71)

Another participant similar sentiments with respect to the Army that reflected parts of H1:

> While I respect the Army as an equal Service, I am concerned that both the Navy and the Air Force are losing their identity due to their absolute saturation in the Army command and the Army way of doing things. (Participant 23)

Whatever the case, the finding that a significant proportion of participants expressed a degree of support for threatening Jointness could be seen to mark a shift away from the strong resistance it has encountered previously.

While no support was found for H1, our results here are intriguing in another respect. Specifically, they indicate that problematic non-disclosure of classified information, this time in the context of request relationships, was likely to surface around Service boundaries. However, just as the results of Study 1 showed that the Service-loyalty effect was qualified by the prospect of formal punishment (i.e., it only emerged when punishment was not expected) our results here do not represent a full and robust Service-loyalty effect. Specifically, Service-loyal disclosure intentions were qualified by the particular course of action participants indicated they would be likely to take. When the requester of classified and 'Service sensitive' information was from within one's Service, participants trusted them more, were more likely to provide the information without delay, were less likely to delay responding, and were less likely to pass responsibility up the chain of command than when the requester

was from another Service. However, Service membership did not affect the likelihood of the participants verifying clearance and/or need to know details, nor seeking advice about how to deal with the request.

While these qualified results do speak to the role of Service affiliation, caution must be taken before concluding that there is something about Service boundaries, *in and of themselves*, that gives rise to problematic non-disclosure of classified information. Specifically, it is possible that by emphasizing the potential for the classified information in question to be "interpreted by other Service personnel" in a way that could harm one's Service, our operationalization of 'Service-sensitive' classified information may have made non-disclosure to other-Service personnel perfectly justifiable. It is also possible that the potency of this prospect eliminated the salience of any Joint identity that emerged beforehand. Thus, it is necessary to test whether problematic non-disclosure of classified and Service sensitive information is still likely to surface around Service boundaries when these justifications are removed from the disclosure scenario, and when the desired social identity (i.e., level of self-categorization) can be expected, beyond reasonable doubt, to be salient.

A final and important point deserves mention. The disclosure scenario employed in Study 2 was one in which the requester had an adequate level security-clearance and, arguably, a legitimate 'need to know' the information requested. In the low-risk condition, the requester belonged to a "Joint area" and asked for the information in the process of preparing a report about how force readiness could be improved. In the high risk condition, the request emanated from an individual in a "Joint area" who was preparing plans for an imminent ADF deployment. Our finding that participants were Service-loyal in many of their disclosure intentions however suggests that the perceived need to know of the requester may have varied according to their Service membership. That, is, own-Service requesters may have been perceived to have a greater need to know the information than other-Service requesters, regardless of what the information was required for. In Study 2, an insight into how, *psychologically speaking*, the requester's Service might influence (at least partly) their need to know is provided by the association between trust in the requester and the various courses of action likely to be taken. Results showed that trust was strongly related to a number of courses of action that might be taken in response to a

request for classified information from both own-and other-Service requesters, notably the likelihood of providing the information without further delay and of passing responsibility for dealing with the request up the chain of command. However, trust (or more accurately a lack of trust) in an other-Service requesters was additionally related to the likelihood that one would verify their security clearance and/or need to know details and seek advice from one's peers about whether to disclose or not. At this point then, it would appear necessary to determine whether perceived need to know does vary with the prevailing social-psychological context, specifically the requester's perceived trustworthiness.

In summary, the findings of Study 2 suggest that Jointness is not likely to constitute a vehicle that undermines Service distinctiveness and in doing so, evoke Service-loyal disclosure outcomes. In other words, problematic non-disclosure around the ADF's Service boundaries do not appear to be driven by a psychological process of Service identity threat. However, this does not imply that social identity processes should be disregarded insofar as gaining an insight into when and why problematic non-disclosure of classified information may surface around Service boundaries. It may be that, rather than being driven by identity threat, problematic non-disclosure emerges from a 'self-categorical gulf' between the potential discloser and recipient. We test this hypothesis in Study 3.

Study 3

Introduction

As outlined above, a core principle of the social identity perspective is that an individual's social identities are *self-categorizations*, that is, they represent categorizations of the self (Onorato & Turner, 2001, 2002; Turner & Onorato, 1999). According to self-categorization theory, when a self-category becomes salient, a process of depersonalization occurs in which the self is perceived as similar and equivalent (i.e., categorically interchangeable) with other ingroup members and different from outgroup group members (Turner et al., 1987). It is the process of depersonalization that is thought to make possible all collective and cooperative behaviour by transforming "my" interests into "our" interests.

In the social identity literature, a considerable amount of work has shown that ingroup favouritism can be reduced by manipulating the level of inclusiveness of the salient self-category, that is, changing who people perceive to be ingroup and outgroup members at any given time (e.g., Dovidio et al., 1997; Gaertner, Mann, Murrell, & Dovidio, 1989; Kessler & Mummendey, 2001). The basic hypothesis common to this work is that ingroup favouritism can be overturned if the salience of the existing "them and us" categorization can be degraded and a new ingroup categorization that includes members of the former outgroup can be made salient (Seta, Seta, & Culver, 2000; see also Gaertner et al., 2000). In these circles, this process is commonly referred to as *recategorization* (Gaertner et al., 1993; Seta et al., 2000).

On the basis of these ideas it could be argued, that like non-cooperation more generally, problematic non-disclosure of classified information may be driven by the perceived ingroup/outgroup memberships that are salient for the potential discloser at the time of their decision-making. Thus, the extent to which problematic non-disclosure of classified information is likely to emerge around Service boundaries could be expected to vary according to whether one's Service represents the salient level of self-categorization when contemplating the disclosure of classified and Service-sensitive information. In this vein, we can conceptualise Service membership as a kind of self-categorical gulf that creates a basis for problematic non-disclosure around Service boundaries. Our intention in this study is to explore the possibility of bridging this self-categorical gulf by making both Services part of the same ingroup. Conventionally, this would be achieved by having group members categorise themselves as belonging to the same superordinate group. In this case however, we propose to bridge this self-categorical gulf by forming an alternative common group membership based on a shared opinion (see McGarty & Bliuc, 2004). Importantly, this shared opinion group membership should be one where the *meaning* of the group and its implied norms convey a sense of common purpose and cooperation. Of course, the same could be implied by making salient the superordinate category "ADF" but as we have established, this superordinate identity is potentially problematic. For example, Navy and Air Force personnel know that are supposed to cooperate with the Army in the context of, say, ADF operations, but they may also

believe that the latter will seek to claim a superior status and dominate them. In other words, there is a pre-existing set of expectations that may impede cooperative disclosure. The alternative proposed here is to craft an identity that should promote cooperative disclosure outcomes. In this case, this would be achieved by defining other-Service requesters as a "supporter" of the potential discloser's Service, that is, as a member of an opinion-based group that is defined by a favourable attitude toward the potential discloser's Service meaning that both discloser and recipient are "on the same team".

Formally, our hypotheses can be summarised as follows:

H1. Perceived need to know and disclosure intentions will be more cooperative when the requester is perceived as an ingroup rather than an outgroup member.

We may also expect:

H2. Perceived need to know and disclosure intentions will be more cooperative when the requester is from one's own Service than from another Service.

Importantly, we also expect there to be an interaction between these factors, in that:

H3. Service-loyal disclosure outcomes will be accentuated when the requester is an outgroup member and attenuated when the requester is an ingroup member.

Also, we can now hypothesize that:

H4. The perceived need to know of the requester will be positively related to the extent to which they are perceived to be trustworthy.

Method

Participants and design

One hundred and ninety-six ADF personnel took part in Study 3. This comprised 82 members of the RAN, 92 members of the ARA, and 22 members of the RAAF. Participants were drawn from Maritime and Land Headquarters (MHQ, LHQ), the Capability Systems Staff (CSS) and the Knowledge Systems Staff (KSS). Again, most were men (87%) and the mean age was 38 years. The majority were of Major equivalent rank or above (78%), with the remainder being of Captain (Army) equivalent rank or below (21%) or of the non-commissioned ranks (1%). Participants had served in the ADF for an average of 19 years and most (76%) held a TOP SECRET security clearance.

The study had a 2 (requester's opinion: supporter/non-supporter) x 2 (requester's Service: own/other) design with both independent variables manipulated between-participants.

Participants were given a questionnaire in which they were presented with a view of their Service and a short scenario which provided the backdrop to a number of questions. The view was an opinion that distinguished "supporters" of the participant's Service by emphasizing those dimensions upon which this Service was respected insofar as its contribution to Australia's defence. Immediately following their responses to the opinion, participants were given a short scenario in which they were asked to imagine receiving a request for certain classified information from another member of the ADF. Following this, they were asked to respond to a number of questions assessing their perception of the requestor (i.e., the potential recipient) and their likely response to the request.

Materials and procedure

Four versions of the study questionnaire were developed, one corresponding to each of the between-subjects conditions (see Appendix C). Each questionnaire was copied on DSTO letterhead and attached was a covering letter which invited

participation in a research program examining the "knowledge environment" of the ADF. The covering letter also stated that participation was voluntary and that all information collected would be anonymous. Questionnaires were randomly distributed to ADF personnel in the participating organizations facilitated by the Chief of Staff or Commanding Officer.

Establishment of the opinion-based group

Written instructions informed participants that there were "competing views" of their Service and that one view which distinguished "supporters" was presented for them below. This view read as follows (questionnaires were matched to participant's Service, the Army example is shown below[11]):

> The Australian Army makes a first-rate contribution toward the defence of our national interests. The complexities of the land environment demand exceptional dedication, expertise, and dependability. The Army has provided, and continues to provide these qualities to the ADF. It has built a reputation for excellence as a land power that is underscored by its values of courage, initiative, and teamwork.

Manipulation of requester's opinion and Service

After responding to the opinion presented above, participants were instructed to imagine a disclosure scenario involving themselves and another member of the ADF known as 'Person X'. This person was either a supporter or non-supporter of the participant's Service and either belonged or did not belong to the participant's Service. The scenario was presented in point form as follows (bracketed terms indicate wording of different conditions, the army example is shown below[12]):

- Person X is a member of the [Army/belongs to one of the other Services], and is working on a report about ADF readiness.

- You know that Person X [is/is not] a supporter of the Army – that is, they genuinely [hold/do not hold] the view of the Army presented earlier.

---

10. Respective Service labels, dimensions (i.e., land/maritime/air) and values varied accordingly.
11. Respective Service labels varied accordingly.

- Person X asks you for classified information about the readiness of some Army force elements (assume you're routinely privy to this information). Person X has the appropriate level security clearance.

- The information that Person X requests contains details about force elements being temporarily at unsatisfactory levels of readiness. The information could damage the image of the Army if not managed with care.

Dependent measures

At the very beginning of the questionnaire, participants responded to three items measuring the extent to which they identified with their Service. These items were identical to those employed in Study 2.

Following the establishment of the opinion-based group, participants were asked to indicate whether they: (1) shared, or (2) did not share this view of their Service. They were also asked to rate the extent to which they agreed with two statements included to increase the salience of membership of the opinion-based group: (1) "I am confident that this view of the [RAN/RAAF/Army] truly captures my own personal beliefs", and (2) "I see myself as a supporter of the [RAN/RAAF/ Army]".

Following the disclosure scenario, participants were asked to respond to 12 questions. The first three questions served as a check of the manipulation of the shared opinion group, that is, whether participants saw Person X as an ingroup member: (1) "To what extent would you feel that Person X respected the [RAN/RAAF/Army]?"; (2) "To what extent would you feel that you and Person X were on the same side?"; and (3) "To what extent would you feel that you and Person X were working toward a common goal?".

Two items served to measure participants' perceptions of Person X's need-to-know: (1) "How legitimate would you consider Person X's 'need to know' the information?", and (2) "How important do you think it is that Person X obtain this information?". One item measured the extent to which participants viewed Person X

as trustworthy in this context: "How confident would you be that Person X would manage this information with care?".

The next five questions mirrored those employed in Study 2 to measure the likelihood of the participant taking various courses of action. Specifically, they were asked how likely they would be to:

(1) "Provide the information to the requester without further delay?" (*disclose*);
(2) "Delay responding to the request until readiness circumstances changed?" (*delay*);
(3) "Go to considerable lengths to verify the requester's security clearance?" (*verify*);
(4) "Seek advice from Service peers about how to deal with the request?" (*advice*);
(5) "Pass the responsibility for handling the request up the chain of command?" (*pass*).

A sixth and final question was added regarding the participant's likelihood of respecting the concerns of Person X if the situation were reversed: (6) "How likely would you be to respect the concerns of Person X if the situation were to be reversed?" (*reciprocate*). Responses to all dependent measures were recorded on 7-point scales with end-points "Not at all" (1) and "Very likely" (7) or the relevant equivalents.

Finally, demographic information including age, sex, rank, length of ADF tenure, and level of security clearance was collected. Participants were then thanked for their time and invited to write comments.

Results

Missing data

There were 11 cases of missing data. In each case, the median score on the item for the sample as a whole was substituted.

Data reduction

There were 18 participants who indicated that that did not share the view that defined supporters of their Service. Additionally, 3 participants failed to respond to the question as to whether they agreed with this view or not. These participants were excluded from further analyses leaving a total sample of 175 participants.

As there was a high degree of inter-item reliability between the three items used to measure participants' identification with their Service, they were collapsed to create a single scale ($\alpha = .86$). A high degree of inter-item reliability was also present between the two items measuring participants' perceptions of the Person X's need to know. Hence, these were collapsed to create a single perceived need to know scale ($\alpha = .92$).

Manipulation checks

Confirming the success of the shared opinion group manipulation, results showed that when Person X was a 'supporter', they were: (1) considered more respectful of the participant's Service than when they were not a supporter (*M*s = 5.47, 3.18; $t(173) = 12.63$; $p < .001$); (2) participants felt to a greater extent they were on the same side as Person X than when they were not a supporter (*M*s = 5.31, 3.55; $t(173) = 8.01$; $p < .001$); and (3) participants felt to a greater extent that they and Person X were working toward a 'common goal' than when they were not a supporter ($M = 5.33, 3.74$; $t(173) = 7.46$; $p < .001$).

Analysis of variance

Scores on dependent variables were submitted to 2 (requester's opinion: supporter/non-supporter) x 2 (requester's Service: own/other) analysis of variance (ANOVA). Means, standard deviations, and *F*-values are presented in Table 6.4

Table 6.4

Means, standard deviations and F-values for dependent measures as a function of requester's Service and requester's opinion.

Requester's Service	Own		Other		*F*-values		
Requester's Opinion	Supporter	Non-supporter	Supporter	Non-supporter	RS	RO	RS x RO
Item (if scale no. items)							
Need to know (2)	5.49 (1.54)	5.14 (1.63)	5.08 (1.60)	4.45 (1.77)	4.82*	3.80*	0.10
Trust	5.64 (1.34)	4.37 (1.56)	4.63 (1.20)	3.44 (1.69)	18.95***	30.29***	0.07
Disclose	5.30 (1.68)	4.97 (1.60)	4.42 (1.65)	4.16 (2.06)	9.72**	1.16	0.28
Delay	2.32 (1.67)	2.74 (1.70)	2.74 (1.71)	2.50 (1.43)	0.14	0.13	0.93
Verify	3.72 (2.31)	4.37 (2.02)	4.26 (2.14)	4.22 (2.13)	0.33	0.86	0.89
Seek	3.70 (2.25)	3.94 (2.04)	4.40 (1.48)	4.42 (2.09)	3.70	0.19	0.04
Pass	3.81 (2.28)	3.71 (2.02)	3.91 (1.54)	4.34 (2.01)	1.43	0.31	1.26
Reciprocate	5.70 (1.08)	4.94 (1.39)	5.12 (1.28)	4.76 (1.61)	3.44	7.25**	1.85

Note: RS = Requester's Service; RO= Requester's opinion
*$p < .05$; ** $p < .01$; ***$p < .001$.

A main effect for the requester's opinion was evident on three dependent measures. The first related to the perceived need-to-know of Person X ($F_{(1,171)} = 3.80$, $p<.05$; $\eta^2 = .02$). Participants rated Person X's need to know as greater when they were a 'supporter' ($M = 5.29$) than when they were a non-supporter ($M = 4.80$). The second effect related to the perceived trustworthiness of Person X ($F_{(1,171)} = 30.29$, $p<.001$; $\eta^2 = .15$) whereby Person X was considered more trustworthy when they were a supporter than a non-supporter ($M = 5.13$; $M = 3.91$, respectively). The third effect related to participants' willingness to respect the concerns of Person X of the situation were reversed ($F_{(1,171)} = 7.25$, $p<.01$; $\eta^2 = .04$). Here, participants were more likely to respect the concerns of Person X if the situation were reversed when Person X was a supporter than when they were a non-supporter ($M = 5.41$; $M = 4.85$, respectively). However, the manipulation of requester's Service did not affect the extent to which

participants were likely to disclose without delay. Thus, only partial support was found for H1.

A main effect for requester's Service was evident on three dependent measures. The first of these related to the perceived need-to-know of Person X ($F_{(1,171)} = 4.82, p<.05; \eta^2 = .03$). Specifically, participants rated Person X's need-to-know to be significantly greater when they were from their own Service ($M = 5.32$) than when they were from another Service ($M = 4.76$). The second effect related to the perceived trustworthiness of Person X ($F_{(1,171)} = 18.95, p<.001; \eta^2 = .10$). Here, participants rated Person X as more trustworthy when they belonged to their Service ($M = 5.01$) than when they belonged to another Service ($M = 4.03$). The third effect related to participants' intentions of providing the information without delay ($F_{(1,171)} = 9.72, p<.001; \eta^2 = .05$). Specifically, participants indicated that they were more likely to disclose the information immediately when Person X belonged to their own Service ($M = 5.14$) than when they belonged to another Service ($M = 4.29$). Thus, support was found for H2.

No significant interactions between the variables were evident and thus, no support was found for H3.

Correlations

In order to examine the relationship between perceived need to know, perceived trustworthiness and the various courses of action, a correlational analysis was performed. Correlations are shown in Table 6.5. The extent to which the requester was perceived to have a need to know was positively correlated with the extent to which they were trusted to manage the information with care. Therefore, support was found for H4. Perceived need-to-know was also highly correlated with the likelihood of disclosing the information with further delay, and negatively correlated with all other courses of action, other than for *reciprocate*. The same pattern was evident for the perceived trustworthiness of the requester, however the correlation coefficients were generally slightly lower.

Table 6.5

Correlations between perceived need to know, perceived trust, and courses of action.

			Course of action					
Item (if scale no. items)	1	2	Provide	Delay	Verify	Advice	Pass	Reciprocate
1. Perceived need to know (2)	---	.63**	.84**	-.44**	-.18**	-.20**	-.40**	.22**
2. Perceived trust		---	.59**	-.35**	-.16*	-.24**	-.27**	.22**

** $p < .01$.

Discussion

The aim of Study 3 was to test the second of our general hypotheses of problematic non-disclosure derived from the social identity perspective. Here, it was argued that like non-cooperation more generally, problematic non-disclosure of classified information is driven by the perceived ingroup/outgroup memberships that are salient for the potential discloser of classified information at the time of their decision-making. Thus, we expected a main effect on disclosure outcomes for shared social identity (H1). Results supported H1 to the degree that when participants perceived the requester of classified information as an ingroup member (i.e., a 'supporter of their Service') they rated them as more trustworthy and were more likely to reciprocate the concerns of the requester if the tables were to be turned. Moreover, participants perceived the need to know of an ingroup requester to be greater than that of an outgroup requester. Yet, perceived ingroup membership did not influence other key dependent measures, particularly the likelihood of disclosing the information to the requester without further delay. Thus only partial support was found for H1. These findings suggest that while a salient and shared identity goes some way to promoting cooperative disclosure outcomes, there is a limit to the extent to which this is likely to be so, as suggested in the comments of one participant:

> If Person X has appropriate clearance (given) and a legitimate need-to-know, there should be no question of withholding information! Their personal view of the RAN should not be an issue. (Participant 145).

We also hypothesized was that a main effect would be observed for the requester's Service (H2). While this hypothesis was not supported across all

dependent measures, it was supported on key measures. That is, when the requester was from one's Service rather than another Service, participants rated them as more trustworthy and as having a greater need to know than when the requester was from another Service. Most importantly perhaps, participants were more likely to disclose the information without delay when the requester belonged to their Service than to another Service. These results mirror those yielded in Study 2 in that a Service-loyalty effect was found on certain courses of action but not others. A parallel can also be drawn here between the size of these effects. For each of the effects listed above, the Service-loyalty effect remained small, just as it did in Study 2. There is arguably a tension within this pattern of results. One the one hand, problematic non-disclosure of classified information appears likely to surface around Service boundaries by impacting the perceived need to know of its potential recipient. On the other hand however, these effects have been shown to be consistently small to date, suggesting that it is not robust and inherent to the ADF.

Our third hypothesis was that the effects for requester's opinion and the requester's Service would interact in that Service-loyal disclosure outcomes would be accentuated when the requester was an outgroup member and attenuated when the requester was an ingroup member (H3). However support for H3 was not found for any of the dependent variables. This findings would appear to confirm the idea that Service-loyal disclosure outcomes are not driven by concerns relating to participants' Service identity. Our final hypothesis was that the perceived need to know of the requester would vary to the extent to which they were perceived to be trustworthy, and be predictive of disclosure intentions (H4). Results supported this hypothesis, providing empirical evidence that perceived need to know did indeed vary according to the prevailing social-psychological context.

General conclusions

On the basis of the two studies presented in this chapter, we must reject the two hypothesis of problematic non-disclosure derived from the social identity perspective in Chapter 5. In so doing, it is now possible to draw some general conclusions about the psychology of problematic non-disclosure in the ADF. First, the findings of Study 2 suggest that Jointness is neither part of the problem and

therefore, nor can it be part of its solution. Second, the findings of Study 3 suggest that problematic non-disclosure of classified information in the ADF does not represent a self-categorical gulf between ADF personnel in terms of their Service identities. Together however, the failure of these studies to adequately account for the psychology of problematic non-disclosure draws attention to a broader and more significant point. That is, it is now possible to conclude that problematic non-disclosure of the form we have investigated here is not driven by personnel's concerns about their Service identity. In other words, the findings of these studies suggest that problematic non-disclosure is not a form of inter-Service rivalry or 'tribalism' driven by issues relating to Service identity.

Having said that, it must be acknowledged that social identification processes may play a limited role in shaping the disclosure environment. Specifically, a shared and salient social identity was found to heighten the perceived trustworthiness of the requester as well as their perceived need to know the information. However, a shared social identity did not influence the extent to which participants in this Study rated themselves as likely to disclose the information to the requester without further delay. Thus, we could conclude that while overtures to a shared social identity may make the general environment more cooperative in nature, they are unlikely to lead to an shift actual disclosure outcomes.

The findings of Study 3 also flesh out arguments made in earlier in Chapter 2 regarding the determination of another's need to know. We have demonstrated in Study 3 that the perceived need to know of the potential recipient of Service-sensitive classified information varies to the extent to which they trust the requester. Additionally, it was also the case that perceived need to know varied in Service-loyal terms, that is, according to whether the potential discloser and recipient belonged to the same Service. At this point, attention must now be directed more fully how both need to know and disclosure intentions are influenced by the second master-factor derived in Chapter 3, that is, perceived risk.

CHAPTER 7

DISCLOSURE AS DECISION-MAKING UNDER RISK:

THE GUARDEDNESS HYPOTHESIS

Introduction

Our early findings suggested that problematic non-disclosure of classified information in the ADF may be likely to surface around the organization's Service boundaries. In Chapter 6, we tested two hypotheses of non-disclosure with this in mind, both derived from the social identity perspective. The first focused on the notion of 'social identity threat' (Branscombe et al., 1999; Jetten, 1999) where it was argued that problematic non-disclosure of 'Service-sensitive' classified information across Service boundaries is driven by a threat to Service distinctiveness evoked by Jointness. According to this hypothesis, a conception of Jointness that undermines Service distinctiveness should accentuate 'Service-loyal' disclosure outcomes while one that highlights Service distinctiveness should attenuate such outcomes. The second hypothesis held that problematic non-disclosure of classified information across Service boundaries reflects a self-categorical gulf between the organization's army, navy, and air force personnel that is salient at the time of the disclosure decision. Here, we expected to attenuate any Service-loyal disclosure outcomes by making salient an alternative self-category that allowed the potential discloser to view a requester from another-Service as an ingroup member.

Only partial support was forthcoming for the hypotheses of Studies 2 and 3. Most importantly, our findings showed that Jointness is unlikely to be part of any non-disclosure problem. However, the extent to which the potential discloser of 'Service sensitive' classified information perceives the potential recipient to be an outgroup member may play some limited role in this phenomenon. Regardless of their Service, an outgroup requester was trusted less than an ingroup member and was seen to have less of a need to know the information than an ingroup member. This latter finding constituted our first piece of empirical evidence showing how the determination of another's need to know classified information will vary according to

the social-psychological context. Yet, our manipulation of social identity in Study 3 had no direct effect on the disclosure intentions of participants. That is, they were no more likely to disclose the information without further delay for an ingroup requester than for an outgroup requester. Our results also showed that a shared and salient social identity was not sufficient to overturn Service-loyal disclosure perceptions and intentions. Our findings indicated that when the participant and the requester were from different Services, the former perceived the latter to be less trustworthy and they were less prepared to disclose to them without further delay than when they were from one and the same Service. Moreover, 'other-Service' requesters were attributed with less need to know the information than 'own-Service' requesters. Thus, at the end of Chapter 6 we were able to conclude that the problematic non-disclosure of the type examined here is not grounded solely in psychological issues concerning Service identity.

In this chapter, we move away from the social identity perspective as an explanatory framework of problematic non-disclosure. Our plan now is to attempt to gain further insights into the psychology of problematic non-disclosure by focusing on the second of the master factors derived from Chapter 3, that is, perceived risk. In the pilot and Study 1, we examined how risk associated with the consequences of *not disclosing* affected decisions about breaching national security. At this point, it is necessary to examine how risk relating to the expected consequences of *disclosing* is likely to affect perception of and responses to requests for Service-sensitive classified information, and if these differ for own- and other-Service requesters.

The purpose of this chapter is to review the theoretical and empirical progress that has been made in psychology regarding risk and its impact on decision-making. Though it is acknowledged, it is not intended here to review the wider literature on risk, that is, the literature beyond the scope of psychology. Instead, our focus here is to cast disclosure and non-disclosure as a type of decision-making, and thus address only the field of 'decision-making under risk'. There are a many theories of decision-making under risk however our focus here will be on three that have held sway in psychology at one time or another: *subjective expected utility theory* (Savage, 1954; von Neumann & Morgenstern, 1944), *prospect theory* (Kahneman & Tversky, 1979), and *regret theory* (Bell, 1982; Loomes & Sugden, 1982). Each spans psychology,

economics, and mathematics, however it is their core psychological hypotheses that are of interest. These hypotheses along with the support they have obtained in studies of decision-making in organizational contexts is reviewed. In order to help us determine what risks ADF personnel are likely to perceive to be involved in the disclosure of classified information to each other, we also turn to the sociological literature on secrecy. The chapter then concludes with a general hypothesis of problematic non-disclosure of classified information in the ADF context.

Decision making under risk: Theoretical & organizational perspectives

Like most psychological concepts, risk suffers from a degree of definitional fluidity (Yates & Stone, 1992). Generally speaking, risk is defined as a type of uncertainty that includes the prospect of loss (Smithson, 1994). Thus, it relates to circumstances where people perceive the consequences of their decision-making to include the probability of negative outcomes - the more negative the outcome, the greater the risk (Vlek & Stallen, 1980; Yates & Stone, 1992). However, the term is also used to refer to *variance* in the probability of outcomes irrespective of whether these outcomes are positive or negative (Forlani & Mullins, 2000; Shapira, 1995). Rather than reflecting the magnitude of the loss, this view sees the more risky decision alternative as the one where the outcome variance is greatest (Lopes, 1987). Both views of risk have enjoyed long histories in psychological theory, primarily within the decision-making (i.e., 'decision-theoretic') literature. For the most part, this literature has been dominated by subjective expected utility theory (Savage, 1954; von Neumann & Morgenstern, 1944).

Subjective expected utility theory

While the term 'expected utility theory' is used to refer a family of decision-making theories that span a number of disciplines, primarily economics, mathematics, and psychology, it is commonly associated with the early work of von Neumann and Morgenstern (1944) and Savage (1954). Fundamental to the theory is the notion of 'utility'. Generally speaking, utility refers to the personal value or *desirability* of the consequences that may arise from a decision in a particular situation (Moser, 1990). For example, a decision to disclose classified information may have consequences that are desirable (e.g., receiving information in return) and those that are undesirable

(e.g., incurring a breach of national security). According to expected utility theory, consequences that are highly desirable are deemed to have higher personal utility than those that are less desirable. The aim of expected utility theory is to infer or reveal utility from people's decisions and preferences (Luce & Raiffa, 1989; Moser, 1990). Hence, the main 'result' of the theory is a utility function that reflects an individual's preferences among various decision alternatives (Luce & Raiffa, 1989).

In expected utility theory, decision-making under risk is a probabilistic affair. That is, a decision is said to be made under risk when the probabilities associated with the various decision outcomes are known (Luce & Raiffa, 1989; Moser, 1990), such as when betting on the toss of a coin where the probability of each outcome is 0.5. In von Neumann and Morgenstern's (1944) articulation of the theory, the probabilities associated with decision outcomes were assumed to be objectively determinable. However, later utility theorists argued against objective probabilities, pointing out that most decision-making takes place in situations where precise outcome probabilities are unknown. Therefore, *subjective* expected utility theory (e.g., Savage, 1954) replaces objective probabilities with subjectively-derived probabilities, arguing that people assign their own probabilities or 'degrees of belief' to the possible outcomes of their decisions (Sawyer, 1990). Either way, risk is conceived as variation in the probability of possible decision outcomes (Forlani & Mullins, 2000; Lopes, 1987; Sawyer, 1990; Shapira, 1995). The core hypothesis of the theory is that people behave *as if* they maximised 'expected utility', that is, the summed product of the utility of each possible outcome and its probability of occurrence (Luce & Raiffa, 1989; Mongin, 1997; Moser, 1990). The theory holds then that, *all other things being equal*, individuals will prefer alternatives with smaller rather than larger risks (March & Shapira, 1987; Shapira, 1995). In other words, people are seen to be generally 'risk-averse' in their decision-making (Lopes, 1987).[13]

Though subjective expected utility theory is rarely mentioned by those seeking to understand how organizational decisions are made, the findings of organizational research often support the theory's general predictions. For example, Dunegan,

12. While the term 'risk averse' is used here to refer to general avoidance of risks, the term is often used to refer more specifically to those who are more avoidant of risk than subjective expected utility theory would predict.

Duchon, and Barton (1992) had members of an international engineering company read a mixed-motive scenario in which they had to decide between keeping an existing and very reliable customer that earned the company a modest income, and dropping the existing customer for a less reliable one that might earn them more, but which had a greater chance of going bankrupt in the process. Participants in this study were asked to rate the degree of risk associated with *declining* the new account and the likelihood that they would pursue it, despite the objections from the existing customer. Not surprisingly, the results indicated that as the perceived risk of *not* taking up the new account increased, the more likely it was to be pursued.

In a similar vein, Forlani and Mullins (2000) sought to examine how different dimensions of risk influenced the decisions of entrepreneurs about whether or not to invest in a new business venture. These researchers manipulated the riskiness of new ventures in terms of the factors outlined earlier, that is, the magnitude of potential loss (low or high) and the variability associated with the predicted outcome (low or high). It was hypothesized that as both dimensions of risk increased, so too would the amount of risk that the entrepreneurs perceived to be associated with the new venture, and that high-risk ventures would be avoided. These hypotheses were supported with one interesting exception. Specifically, Forlani and Mullins found that their sample of entrepreneurs showed a tendency to prefer high-hazard ventures, that is, those in which the magnitude of potential loss was high. To explain these results, the researchers argued that high-risk ventures may be attractive as long as the prospect of commensurate gains are sufficiently likely. However, an alternative explanation may be found in the work of March and Shapira (1987; see also Shapira, 1995). Based on a large survey of business managers, these researchers found that managers were willing to take large risks if they perceive themselves to be able to exercise some degree of *control* over the possible outcomes. Indeed, in follow-up research by Forlani (2002), this very hypotheses was supported in a study of investment decision-making.

As illustrated above, people are well known for not always avoiding what appear to be large risks. Indeed, classical economists remain vexed by the fact that the people behave as if they are risk-averse in some circumstances (e.g., purchasing house insurance) and risk-seeking in others (e.g., purchasing lottery tickets; see

Lopes, 1987). One of the best-known theoretical analyses that attempts to account for certain inconsistencies of this kind is prospect theory (Kahneman & Tversky, 1979).

Prospect theory

Prospect theory (Kahneman & Tversky, 1979; see also Kahneman & Tversky, 1982) is a theory of decision-making under risk developed to account for certain violations of expected utility theory. As outlined above, the latter maintains that the overall utility of a decision alternative is the expected utility of its outcomes and that people are generally risk-averse in their decision-making. However, Kahneman and Tversky observed that the expected utility of a decision alternative was usually assessed in relation to a reference point, generally the status quo. Moreover, they observed that by varying the way a decision problem was 'framed', that is, whether the decision represented the prospect of a loss or a gain, people would be either risk-averse or risk-seeking in their choices. To demonstrate this, Kahneman and Tversky typically presented individuals with a set of decision problems in which they had to choose between two alternatives, A and B. One option (A) represented a risk-seeking choice while the other (B) represented a risk-averse choice. Further, the decision situation was presented in either a 'gain frame', for example:

Which of the following would you prefer?

A: 50% chance to win $100
50% chance to win $0;

B: Win $45 for sure.

or a 'loss frame', for example:

Which of the following would you prefer?

A: 50% chance to lose $100
50% chance to lose $0;

B: Lose $45 for sure.

The results of studies like these indicated that people tended to be risk-averse when faced with the prospect of a gain (i.e., they tend to take the 'sure thing'). Yet, when faced with the symmetrical gamble framed as a loss, people tended to be risk-seeking, that is, they tended to 'chance their hand' in the hope of avoiding any loss. According to prospect theory then, an individual's value function (utility was redefined as value)

depends on whether one is facing potential gains or potential losses. In other words, people's risk-taking behaviour is shaped in large part, by the *context* of the decision situation.

Applied research has yielded some support for the idea that perceptions of risk are influenced by context. It is argued, for instance, that the prevailing context makes certain dimensions of risk more salient than others (Fischhoff, Watson, & Hope, 1984; Forlani & Mullins, 2000; March & Shapira, 1987; see also Vlek & Stallen, 1980; Yates & Stone, 1992). Specifically, the *probability* of loss may be important in situations where its magnitude is small and the probabilities are well specified. However, the *magnitude* of loss may be more important in circumstances where the loss is considerable in size and its probability is difficult to assess (Vlek and Stallen, 1980). Yet, direct support for prospect theory is evident in the findings of much organizational research (see Fiegenbaum & Thomas; 1988, Hoskinsson, Hitt, & Hill, 1991; MacCrimmon & Wehrung, 1986; March & Shapira, 1987; Shapira, 1995). A common theme in this research, for instance, is that company managers are generally unwilling to take risks when their companies are performing well and there is little danger of falling behind performance targets (i.e., when in the 'domain of gains'). Yet, when one is in danger of missing performance targets or when the company's actual survival is at stake (i.e., when in the domain of losses), riskier options become more attractive. This focus on the psychology of potential gains and losses draws attention to the impact that emotions have on decision-making under risk[14]. Theoretically, this area has been dominated by regret theory (Bell, 1982; Loomes & Sugden, 1982) in which the concept of 'anticipated regret' is employed to explain phenomena such as risk-aversion and so-called 'sunk-cost' effects (see Connolly & Zeelenberg, 2002).

Regret theory

By referring to people's emotional experiences, the aim of regret theory is to offer an alternative model of decision-making under risk. The historical roots of regret theory can be traced at least as far back as Savage (1954) and Luce and Raiffa

13. See Mellers, Schwartz, & Ritov (1999) for a brief overview review of emotion-based theories of choice.

(1957) who argued that prior to decision-making, people compute their maximum possible regret for each decision alternative and then choose the alternative where this maximum is the lowest - the so-called *minimax principle of regret* (Mellers, et al., 1999; Zeelenberg, 1999). In later years, Janis and Mann (1977) argued that people will seek to ensure their decision-making is of high quality if they think beforehand about possible regret. However, Bell (1982) and Loomes and Sugden (1982) were the first to devise a formal psychological theory of decision-making under risk in which the notion of anticipated regret was central (Sugden, 1985).

Two emotions are core to formal regret theory: *regret* and *rejoicing* (Sugden, 1985). Regret is the negative feeling that emerges when the outcome of one's actual decision is worse than that which would have been obtained if one had chosen differently (e.g., discovering that the lottery ticket one refused turns to be out the winner). Rejoicing is the feeling that emerges when one discovers that the outcome of their actual decision was, in fact, the best outcome (e.g., finding out that the train one did not take had broken down). While regret and rejoicing are *post-decisional* experiences, regret theory holds that they have a strong *pre-decisional* influence on decision-making in that they are anticipated when a decision-maker is faced with a choice between risky options (Zeelenberg, 1999). Specifically, it is assumed that decision-makers wish to minimize post-decisional regret (Connolly & Zeelenberg, 2002; Zeelenberg, 1999). Thus, according to regret theory, people will be risk-averse when the 'risky' choice is the one that makes post-decisional regret salient, and will be risk-seeking when it is the more certain alternative that may lead to greater levels of post-decisional regret (see Zeelenberg, 1999).

Empirical support for regret theory has been mixed (see Loomes, Starmer & Sugden, 1992; Zeelenberg, 1999). Support is offered by Simonson (1992) who found that people's purchasing decisions could be varied by making salient the level of regret they would experience if their choice were to turn out badly. Here, high levels of anticipated regret influenced people to buy a more expensive and reliable brand

product than a cheaper and more risky one. Yet, the regret-rejoicing process has not received extensive attention in studies of organizational decision-making[15].

Summary and implications

So far, we have reviewed three theories of decision-making under risk that have held sway in the psychological literature at some time or another: subjective expected utility theory (Savage, 1954; von Neumann & Morgenstern, 1944), prospect theory (Kahneman & Tversky, 1979) and regret theory (Bell, 1982; Loomes & Sugden, 1982). We have also briefly reviewed the extent to which support for the core ideas of these theories has been found in studies of organizational decision-making. It would now be possible therefore to propose general statements about the psychology of problematic non-disclosure for each of the theoretical frameworks reviewed. For instance, it could be argued that non-disclosure simply maximises expected utility. Or, from the point of view of prospect theory, it could be said that non-disclosure is the alternative that provides the potential discloser with a chance of avoiding certain loss. Finally, a regret theorist might argue that non-disclosure is associated with lower levels of anticipated regret.

While such statements represent the potential discloser as a decision-maker operating under risk, they fail to answer a question of the central importance: why is it that not-disclosing rather than disclosing maximises expected utility, avoids certain loss, or minimizes post-decisional regret? In other words, neither the theoretical nor the empirical work reviewed above sufficiently addresses why the disclosure of classified information amongst ADF personnel should be considered a risky activity. Furthermore, the work offers no insight into the reasons why intra- or inter-Service disclosure should be seen as the riskier option. It is now necessary to step outside the psychological literature for an insight into the answer to these questions. We therefore turn to the sociological literature relating to secrecy.

---

14. To some extent, many of the findings reported above could be argued to be consistent with regret theory, however little or no reference is made within these studies to the emotional experiences (anticipated or otherwise) of participants in general.

The contribution of sociology and the guardedness hypothesis

In Chapter 3, we saw how perceived risk has long been associated with non-disclosure of personal information. More specifically, a major theme running through psychological analyses of self-disclosure is that the revelation of personal information is risky because its leaves the potential discloser vulnerable to the unknown intentions and perceptions of the potential recipient (Kelly, 2001; Margulis, 1977; Petronio, 1999). Similar ideas are also evident in the sociological literature that relates to the dynamics of organizational secrecy. However in the sociological literature, a distinction can be made between two traditions within this research.

In the first tradition, risk is seen as an *external* factor shaping the organization from the outside. In other words, the organization is vulnerable to threats emanating from beyond its boundaries and these threats justify a need for information control systems to be developed in order to protect the organization (Erickson, 1979). This idea can be traced back to Simmel who, in discussing the structure of the secret society argued that "the purpose of secrecy is, above all, protection" (Simmel, 1950, p. 345). The use of secrecy for protection from external threats and risks is obviously important in defence organizations where elaborate forms of information control function, first and foremost, to conceal a nation's defence arrangements (i.e., its weaknesses and advantages) from outsiders perceived to have malicious intents (Bok, 1984; Lowry, 1972; Wilsnack, 1980). As suggested by Bok (1984), the unrelenting presence of an external source of risk appears to permeate the psyche of military personnel in a way that orients them inward and away from their counterparts in civilian life:

> To insiders, the dangers of ill-advised disclosure seems greater than that of ill-advised secrecy...To live with secrecy day in and day out, to be aware of a threat to both one's nation and to oneself from a diminution of secrecy, and to be trained to give up ordinary moral restraints in dealing with enemies is an experience that isolates and transforms participants (pp. 198-99).

In the second tradition, risk is viewed as an *internal* factor and therefore one capable of shaping the relations amongst an organization's personnel from the inside. Work in this tradition converges on the idea that risks within the organization make

organizational secrecy an inherently unstable form of information control (Bok, 1984; Lowry, 1972; Wilsnack, 1980). Moreover, these internal risks are seen as fundamental to why disclosure outcomes within the organization may not always be commensurate with those envisaged by formal rules and procedures (Erickson, 1979). Hence, a major theme in this work is 'organizational paranoia'. That is, instead of looking outward for sources of threat, an organization's members turn their suspicions toward one another and these manifest as dysfunctional patterns of non-disclosure. Again, Bok (1984) captures the essence of this idea:

> It is no wonder that military secrecy offers fertile ground for pathological disturbances. The fear of betrayal - seeing enemies everywhere, fearing pervasive conspiracies and hidden designs - flourishes under conditions of external threat between nations. And the secrecy sought in response to such fears begins to seem more and more like a conspiracy in its own right, as it spreads and erodes rationality (pp. 199).

Perhaps the most significant sociological contribution in this vein is that made by the functionalist Edward Shils (1956) in *The Torment of Secrecy.* In his analysis of McCarthyism, Shils observed that the mere possession of an official secret during this era gave rise to the suspicion of disloyalty, in this case, to one's country. Significant also are Lowry's (1972) self-reports while employed by a U.S. Army 'think-tank'. Here, Lowry observed that official secrecy served not only to protect national security but to restrict politically sensitive information from reaching others within the organization deemed to be a political threat (see also Wilsnack, 1980). Along similar lines, Aftergood (2000) recently differentiated three categories of secrecy as practiced by defence organizations (1) genuine national security secrecy, (2) bureaucratic secrecy (i.e., secrecy conducted for the sake of secrecy without any real national security implications) and (3) political secrecy, or the deliberate non-disclosure of classified information to gain political advantage or avoid political embarrassment.

A second, more subtle theme also runs through work in this tradition, in this case, one of guardedness. Here, non-disclosure of valuable information is seen as a response to fear and uncertainty about how the information might be used 'down the line'. This idea is well illustrated by Erickson (1979). Working from a conflict framework (see Dahrendorf, 1968), Erickson argues that the perceived need for

secrecy is based on fear and uncertainty as to how others would use valuable information if it happened to be disclosed to them. Specifically, Erickson argues that organizations in which secrecy is perceived to be necessary are dominated by norms of distrust rather than norms of rationality, pointing out that:

> One can judge others as enemies who are intentionally interested in subverting one's aims and the past history of their actions can serve as a basis for arriving at such a judgement. But one can also judge others as stupid or careless and therefore fear what would happen if certain information were made available to them. These reasons for fearing others have as their central core feature an evaluation of the untrustworthiness of others (p. 126).

A sense of guardedness is also evident in recent analyses of the intelligence-sharing arrangements amongst the agencies of the U.S. Intelligence Community prior to September 11, 2001 (see United States House Committee, 2002). As alluded to in Chapter 2, intelligence collectors often restricted the access of intelligence analysts to sensitive information because of fears that the latter might use the information in a way that exposed the source, that is, the actual technique or person that acquired the information. These fears were found to have reinforced inappropriate norms of 'ownership' over sensitive information. According to Admiral Thomas Wilson, a former director of the CIA, perceived ownership of information represented a significant cultural concern and that agencies need to "shed the belief that they own information, which, in fact, belongs to the government" (United States House Committee, 2002, p. 363).

Based on the work conducted within this latter tradition, we can derive a general hypothesis of problematic non-disclosure of classified information in the ADF that could be termed 'the guardedness hypothesis'. According to this hypothesis, perceived risk as to how the requester of Service-sensitive classified information might use the information if disclosed is central. Specifically, problematic non-disclosure of the form examined here is argued to represent a guardedness that is aroused by uncertainty as to whether the requester and/or the recipient of subsequent disclosures will use the information in a way that is harmful to one's Service. Further, the guardedness hypothesis could be extended so as to argue that such guardedness will be accentuated when the potential recipient is from another Service. According

to the ideas reviewed above, we could expect members of 'other' groups to be malicious or careless with sensitive information about one's own group and that one must be most cautious when deciding whether to disclose such information to these 'outsiders'.

Summary and the way ahead

We began this chapter by reviewing the major theoretical contributions that have been made in psychology concerning decision-making under risk. Of the many theories of this kind, three were outlined together with evidence in support of their hypotheses. While it is possible to derive a number of general statements about the psychology of problematic non-disclosure in line with each of these theories, such an exercise is inadequate for our purposes in one important respect. Specifically, neither the theories of decision-making under risk nor contemporary organizational research in this vein are able to shed any light on why the disclosure of classified information as it takes place amongst ADF personnel should be considered a risky activity nor why inter- or intra-Service disclosure should be considered the more risky option.

In order to gain such an insight, it is necessary to examine how risk and non-disclosure have been associated in sociological analyses of secrecy. In this literature two distinct traditions were discerned. In the first, risk is viewed as a factor that shapes the organization from outside thus orienting its members inward. However, it was argued that the second tradition is the more important. Here, risk is viewed as something that resides *within* the organization relating to how other insiders might use valuable information if it is disclosed to them. On the basis of this idea, we hypothesized that problematic non-disclosure of Service-sensitive information in the ADF represents a form of guardedness or circumspection driven by uncertainty as to how disclosed information might be used by the requester or those the requester may disclose the information to. The following chapter is to test this idea empirically.

CHAPTER 8

TESTING THE GUARDEDNESS HYPOTHESIS

Introduction

In the previous chapter, our attention shifted toward risk, the second of the two master factors derived from the review of disclosure conducted in Chapter 3. Chapter 7 summarised three of the major theoretical approaches to risk in the psychological literature and reviewed the extent to which the arguments and assumptions of these theories are reflected in studies conducted within an organizational context. Like research conducted in the social identity tradition, studies of organizational decision-making under risk have yet to adopt disclosure and non-disclosure as dependent variables of major research interest. Therefore, in order to gain some insight into how risk might underpin problematic non-disclosure in the ADF and why inter- or intra-Service disclosure should be seen as the riskier option, it was necessary for us to turn to sociological accounts of organizational secrecy where perceived risk is a central theme (e.g., Coser, 1963; Erickson, 1979; Lowry, 1972; Shils, 1956; Wilsnack, 1980).

On the basis of the arguments presented in the sociological literature, we concluded Chapter 7 by proposing what we have termed the *guardedness hypothesis*. This hypothesis holds that problematic non-disclosure of Service-sensitive classified information is a protective response to perceived risk. More specifically, it is argued that problematic non-disclosure of the form examined here represents a cautiousness or circumspection aroused by perceived uncertainty as to whether the requester (or those the requester may subsequently disclose the information to) will use the information in a way that harms the potential discloser's Service. Further, it was suggested that the hypothesis could be extended so as to argue that any guardedness in one's perceptions and intentions to disclose would be accentuated when the potential recipient of the information belongs to another Service. Those from other groups, it was argued, being more likely to be the ones that are careless or ignorant to the sensitivities embedded within such information.

The aim of this chapter is to test the guardedness hypothesis and two studies are conducted to that end. The purpose of Study 4 is to provide an initial validation of the ideas central to the hypothesis in the ADF context. More specifically, the goal here is to demonstrate using a simple survey that the disclosure of classified information both within and across Service boundaries is likely to be associated with various risks relating to the potential recipient's use of the information. Further, we seek to also demonstrate that the determination of another's need to know is likely to be associated with one's level of confidence about (i.e., toward) these risks. In Study 5, the aim is to test the guardedness hypothesis more directly, seeking causal rather than correlational associations. Specifically, the goal of Study 5 is to determine whether perceived risk as to how the classified information might be used causes participants to be cautious in attributing to own- and other-Service requesters a need to know the information and in deciding to disclose to them without delay. To that end, we manipulate the extent to which study participants feel as though they are able to control how own- and other-Service requesters might use Service-sensitive classified information they disclose. Thus, this study draws on organizational research which suggests that perceived control moderates one's reluctance to choose risky options (Forlani, 2002, March & Shapira, 1987; Shapira, 1995). In an effort to flesh out the variability in Service-loyalty across all thesis studies, the chapter concludes by providing a number of illustrative excerpts from qualitative data collected by way of interviews and experimental questionnaires.

Study 4

Introduction

Core to the guardedness hypothesis is the idea that the disclosure of sensitive information carries with it a risk that it will be misused by the recipient (or those the recipient may subsequently disclose to) either deliberately or accidentally. This broad class of risk arguably potentially contains a number of subclasses that may be important drivers of non-disclosure, either independently or in combination. For example, guardedness in one's disclosure intentions may be driven primarily by a perceived inability to predict or anticipate how Service-sensitive information will be used if disclosed. Additionally, it may emanate from an expectation that the potential

recipient of the information will not recognise and/or manage any risk to one's Service that is inherent in the information. Alternatively, it may be the case that the potential discloser of the information is primarily concerned with the consequences they face if disclosing turns out to be the 'wrong' decision. In other words, the guardedness in one's disclosure intentions may stem from the perceived risk of being held personally responsible for any damage to one's Service that might occur post-disclosure. Finally, it may be that the risks relate largely to the prospect of disclosing to people that one does not know personally.

As outlined above, the aim of Study 4 is twofold. First, our goal is to demonstrate that the disclosure of classified information in both intra- and inter-Service contexts is likely to be associated with various risks relating to the potential recipient's use of the information, such as those that have been outlined above. Second, we seek to demonstrate that the extent to which personnel feel confident about these risks is likely to affect their judgment of the recipient's need to know the information. To this end, it was decided to conduct Study 4 as a simple survey in which ADF personnel are asked to rate their level of confidence toward risks such as those described above in addition to their level of confidence regarding their ability to determine need to know. The primary purpose of Study 4 is to demonstrate the associations that are core to the guardedness hypothesis and we can expect that:-

H1: The more confident that ADF personnel are about the risks associated with disclosing classified information, the more confident they will be about determining need to know.

Based on prior results, we might also expect that:

H2: ADF personnel will be more confident about the risks associated with disclosing classified information in intra- rather than in inter-Service contexts.

Method

Participants and design

Thirty ADF personnel drawn from the Deployable Joint Force Headquarters (DJFHQ) took part in Study 4. This comprised 23 men and 7 women, all belonging to the ARA. The majority were commissioned officers with 7 of Major rank or above and 11 of Captain (Army) rank or below. The remaining 12 were non-commissioned officers. The mean age was 36 years and average length of ADF service was 16 years. Most held a TOP SECRET security clearance (n = 22).

The survey was designed to measure the general level of confidence of ADF personnel with respect to various risks associated with disclosing classified information in intra- and inter-Service contexts. It had a 2 (disclosure context: intra- versus inter-Service) x 6 (class of risk) design with both factors manipulated within-participants.

Materials and procedure

Each survey was copied on DSTO letterhead and attached to a covering letter that invited participation in a research program that examined the "knowledge environment" of the ADF (see Appendix D). The covering letter also stated that participation was voluntary and that information collected would remain anonymous. Questionnaires were distributed with the assistance of the Chief of Staff.

Instructions at the beginning of the questionnaire informed participants that the aim of the questionnaire was to examine what ADF personnel thought about the provision of classified information to each other, and that they would be asked to rate how confident they were about a number of issues relating to the disclosure of classified information within and across Service boundaries. These instructions read as follows:

> On the next page, you will be asked to **rate how confident you would be** about a number of issues involving the disclosure of classified information in the ADF. Each question requires that you respond twice.
>
> That is, on the left hand side of the page, you are asked to respond keeping in mind disclosure that takes place across Services. And, on the right hand side, you are asked to respond to the same question, but this time keeping in mind disclosure that takes place completely within your Service.

Ordering of the disclosure context was counterbalanced and questionnaires were distributed to personnel on a random basis.

Dependent measures

For each disclosure context, personnel were asked to rate how confident they were with respect to six different issues, each of which represented a potentially risky aspect of disclosing classified information. Specifically, participants were asked how confident they were:

(1) "about being able to determine 'need-to-know'?" *(need-to-know)*
(2) "about being able to anticipate or predict how the disclosed information might be used?" *(prediction)*
(3) "that risks to your Service associated with disclosing will be **recognised** by the recipient(s)?" *(recognition)*
(4) "that risks to your Service associated with disclosing will be **managed** by the recipient(s)?" *(management)*
(5) "that you would not be seen as 'personally responsible' if classified information you disclosed was used by others in a way that damaged the image of your Service?" *(blame)*
(6) "about disclosing classified information about your Service to recipient(s) you don't know personally?" *(unknown)*

Responses to all six classes of risk were recorded on 7-point scales with end-points labelled "not at all" (1) and "very confident" (7) and headed either "*Disclosing within my Service*" or "*Disclosing across Services*".

Finally, demographic information including age, sex, rank, level of security clearance, and years of ADF service was collected. Participants were then thanked for their time and invited to provide comments.

Results

Missing data

There were three cases of missing data. In each case, missing data was substituted with the median of the relevant variable for the sample as a whole.

Correlational analysis

For each disclosure context, correlations between all dependent measures were calculated and are shown in Table 8.1. We found support for H1 with respect to both intra- and inter-Service disclosure contexts. In intra-Service contexts, the extent to which participants felt confident about determining need to know was associated with their level of confidence across all other classes of risk, particularly that relating to being able to predict how disclosed information might be used. In inter-Service contexts, this pattern was mirrored to a large degree. There was one difference here in that confidence about determining need to know in inter-Service contexts was not related to confidence about disclosing to personnel (in this case, those from other Services) that one did not know personally. Indeed, in the inter-Service disclosure context, participants' level of confidence about disclosing to those they did not know personally was not related to their confidence toward any other class of risk.

Analysis of variance

Scores for the dependent measures were submitted to a 2 (disclosure context: intra/inter-Service) x 6 (class of risk) within-participants ANOVA. Means and standard deviations for dependent measures are shown in Table 8.2. ANOVA statistics are shown in Table 8.3.

Table 8.1

Inter-correlations between dependent measures for intra- and inter-Service contexts.

Class of risk	1	2	3	4	5	6
			Intra-Service disclosure			
1. Need to know	--	.66**	.42*	.50**	.37*	.42*
2. Prediction		--	.49**	.58**	.50**	.56**
3. Recognition			--	.87**	.40*	.39*
4. Management				--	.52**	.40*
5. Blame					--	.35
6. Unknown						--
			Inter-Service disclosure			
1. Need to know	--	.82**	.54**	.60**	.54**	.19
2. Prediction		--	.53**	.58**	.46**	.25
3. Recognition			--	.92**	.51**	.18
4. Management				--	.61**	.15
5. Blame					--	.36
6. Unknown						--

*$p < .05$; ** $p < .01$; ***$p < .001$

Table 8.2

Means and standard deviations for dependent measures for intra- and inter-Service disclosure contexts.

	Disclosure context	
Item	Intra-Service	Inter-Service
Need to know	5.87 (0.97)	4.50 (1.53)
Prediction	5.47 (1.07)	3.87 (1.53)
Recognition	5.17 (1.34)	3.57 (1.57)
Management	5.00 (1.49)	3.43 (1.59)
Blame	3.60 (2.18)	3.00 (1.95)
Unknown	3.93 (2.07)	2.83 (1.90)

Table 8.3

ANOVA statistics for classes of risk as a function of disclosure context.

Source	*df*	*F*	η^2	*p*
Disclosure context (D)	1	45.54	.61	.000***
Class of risk (C)	5	12.47	.30	.000***
D x C	5	5.73	.17	.000***

***$p<.001$;

We found support for H2 in that results indicated a main effect of large size for disclosure context ($F_{(1,29)} = 45.54, p<.001$). Specifically, participants were more confident about disclosing classified information in intra-Service rather than in inter-Service contexts (*M*s = 4.84, 3.53 respectively). Results also indicated a main effect of moderate size for class of risk in that participants' confidence varied across the classes of risk presented ($F_{(5,145)} = 12.47, p<.001$). Estimated marginal means are shown in Table 8.4.

Table 8.4

Estimated marginal means for confidence about class of risk

Class of risk					
Need-to-know	Prediction	Recognition	Management	Blame	Unknown
5.18_a	4.67_b	4.38_b	4.22_b	3.30_c	3.38_c

Means not sharing any subscript differ significantly at p<.05 or less.

Participants were most confident about their ability to determine need to know, yet were only moderately confident about being able to anticipate or predict how the recipient of classified information would use this information, and that the recipient would recognise and manage any risks to one's Service inherent in the information. The lowest levels of confidence were in respect to the expectation that one would not be seen as personally responsible if information they disclosed was later used by others in a way that damaged the image of their Service, and about disclosing classified information about one's Service to unknown others.

There was also an interaction between disclosure context and class of risk of small effect size ($F_{(5,145)} = 5.73, p<.001$) indicating that the disclosure contexts yielded significantly different disclosure confidence profiles as shown in Table 8.5.

Table 8.5

Means for dimensions of disclosure confidence: Intra- and inter-Service contexts

	Class of risk					
Context	Need-to-know	Prediction	Recognition	Management	Blame	Unknown
Intra-Service	5.87_a	5.47_b	$5.17_{b,c}$	5.00_c	3.60_d	3.93_d
Inter-Service	4.50_a	3.87_b	$3.57_{b,c}$	$3.43_{b,c}$	$3.00_{c,d}$	2.83_d

Means not sharing any subscript differ significantly at p<.05 or less.

The only difference between the two disclosure confidence profiles related to participant's level of confidence that they would not be seen as personally responsible if information they disclosed was used by others in a way damaging to their Service (*blame*). For the intra-Service context, mean scores for *blame* were significantly lower than all other means except for *unknown*. However, for the inter-Service context, mean scores on *blame* did not differ significantly from those on *recognition* and *management*.

Discussion

The aim of Study 4 was to provide an initial and broad validation of the ideas central to the guardedness hypothesis in the ADF context. Specifically, the primary purpose of this study was to demonstrate that the disclosure of classified information both within and across Service boundaries is likely to be associated with various risks relating to the potential recipient's use of the information. The findings of Study 4 speak to this objective in that our participants were readily able to rate and differentiate their level of confidence about various issues relating to disclosure of classified information that are core to the hypothesis. When the disclosure context was intra-Service in nature, participants were moderately confident about their ability to predict how disclosed information would be used, as they were that the recipient of

such information would recognise and manage any risks to their Service inherent in the information. However, for an inter-Service disclosure context, participants were far less confident in these respects.

We expected in Study 4 that participant's level of confidence towards the risks associated with disclosing classified information would vary directly with their level of confidence about determining need to know (H1). We found support for this hypothesis for both the intra- and inter-Service disclosure contexts. In short, the more confident that participants were about the various risks, particularly about being able to predict how disclosed information might be used, the more confident they were about their ability to determine need to know. There was one interesting exception in that participants' confidence about being able to determine need to know was not related to their confidence about disclosing to unknown others when these unknown others were from outside one's own Service. It would appear then that the most salient risks associated with inter-Service disclosure are not to do with the potential recipient being unknown to the potential discloser, but with more broader issues relating to predictability and the recognition and management of risk to one's Service.

We also expected that participant's level of disclosure confidence would be greater when contemplating intra- rather than inter-Service disclosure (H2) and this hypothesis too was supported. Indeed, the size of this Service-loyalty effect was somewhat larger than had been observed in our prior studies. It is possible that this is due to the particular sample of personnel that took part in Study 4. While DJFHQ is officially a 'Joint' organization, the majority of personnel of this Headquarters and indeed all of those who took part in Study 4, belong to one Service, in this case, the ARA. These results provide support for the extension of the guardedness hypothesis outlined earlier, specifically, that the potential discloser of classified information that is sensitive to one's Service will likely be more cautious in disclosing it to other-Service personnel than to own-Service personnel.

In summary, the findings of Study 4 provide an initial validation of the ideas central to the guardedness hypothesis. Moreover, they go some way toward showing that the extent to which the potential discloser of classified information is confident toward disclosure risk is likely to be a salient factor in the determination of another's

need to know the information. However, the correlational nature of this data means that causal relationships remain uncertain. It is not clear, in other words, whether the risk associated with the inability to anticipate how the recipient will use the information *causes* personnel to rate need to know as lower and to be more reluctant to disclose classified information without delay. The aim of Study 5 is to investigate whether this causal association. Specifically, our goal is to investigate the whether it is possible to systematically change one's perceptions of a requester's need to know by varying the extent to which the disclosure situation is perceived to be risky, in this case, in terms of how the requester might use the information if disclosed. Central here is the extent to which the potential discloser perceives that they can *control* how the requester will use the information (see Forlani, 2002). Specifically, we expect the following:-

H1: When participants believe that they can exert such control, they will perceive the disclosure situation to be less risky than when they believe that they cannot exert such control, and

H2: When participants believe that they can exert such control, they will attribute to the requester a greater need to know and be more willing to disclose without delay than when they believe that they cannot exert such control.

Based on the results of prior studies, we could also expect Service-loyal outcomes. Specifically:-

H3: When participants are from the same Service as the requester, they will perceive disclosing to be less risky, attribute a greater need to know to the requester, and be more willing to disclose without delay, than when they are from a different Service.

However, it could also be expected that:-

H4: The Service-loyalty effects of H3 will be accentuated when participants believe that they can exert control over the requester, and attenuated when they believe that they cannot exert such control.

Study 5

Method

Participants and design

Ninety-six ADF personnel from HQNORCOM, AHQ, NHQ and AFHQ took part in the study. This comprised 74 men and 18 women (4 participants did not indicate their sex). Of these, there were 46 ARA personnel, 23 RAN personnel, and 27 RAAF personnel. The majority (n = 63) were commissioned officers with 43 of Major-equivalent rank or above and 20 of Captain (Army)-equivalent rank or below. The remaining 30 participants were non-commissioned officers (3 participants did not indicate their rank). The mean age was 37 years, and average length of ADF service was 17 years. The vast majority (n = 67) held a TOP SECRET security clearance.

The study had a 2 (perceived control: low/high) x 2 (requester's Service: own/other) design with both independent variables manipulated between-participants.

Participants were given a questionnaire in which they were told that a short scenario provided the backdrop to a number of questions. In the short scenario, participants were asked to imagine receiving a request for a certain piece of classified information from another member of the ADF. Following this, they were asked to respond to a number of questions assessing their perception of the requester and their likely response to the request.

Materials and procedure

Four versions of the study questionnaire were developed, one corresponding to each of the between-subjects conditions (see Appendix E). Each questionnaire was copied on DSTO letterhead and attached to a covering letter that invited participation in a research program examining the "knowledge environment" of the ADF. The covering letter also stated that participation was voluntary and that all information collected would remain anonymous. Questionnaires were randomly distributed to

ADF personnel in the participating organizations, facilitated by the respective Chief of Staff or Commanding Officer.

Upon opening the questionnaire, participants were instructed to read the following scenario (RAAF version shown, bracketed terms indicate wording used to match questionnaires to participant's Service)

> Imagine that you are routinely privy to classified information about the capability level of RAAF force elements as part of your normal duties.
>
> On this occasion, you are approached by a member of [the RAAF/another Service] who is preparing a report concerning ADF preparedness. For the purposes of this report, this person, whom you don't know personally, requests that you provide classified information regarding the current capability level of certain RAAF force elements.
>
> The information requested contains details about force elements being temporarily at unsatisfactory levels of capability and if not managed with care, could damage the image of the RAAF.

Manipulation of perceived outcome control

In the low perceived control condition, the scenario concluded with:

> The requester, who is appropriately cleared, reminds you that you will not be able to view the report before it is completed and disseminated.

In the high perceived control condition, the scenario concluded with:

> The requester, who is appropriately cleared, provides a guarantee that you will be able to check the report before it is completed and disseminated.

Dependent measures

To check the manipulation of perceived control, participants were asked the following: "To what extent would you feel you could control how the requester used the information?".

Following this, participants were asked to respond to 7 questions relating to the disclosure situation generally, their perception of the requester, and their likely response to the request. Four items served to assess the extent to which the requester perceived the disclosure situation as risky (bracketed terms indicate wording used in different conditions):

(1) "To what extent would providing the information without delay be risking the [Army's/RAAF's/RAN's] image?" (*image)*;
(2) "To what extent would providing the information without delay be risking your professional reputation?" (*reputation)*;
(3) How confident would you be that the requestor would manage any risks to the image of the [Army/RAN/ RAAF]?"; (*manage*)
(4) "If you were to provide the information to the requestor without delay, how confident would you feel that the final report would treat the [Army/RAN/ RAAF] fairly?". (*fairness*)

Along similar lines to the measures used in Study 3, two items served to measure participants' perception of the requester's need to know: (1) "To what extent would you think the requestor has a 'need to know'?"; and (2) "To what extent would you think it important that the requestor obtain the information?". In line with our previous studies, a final item served to assess participants' disclosure intentions: "How likely would you be to provide the information to the requester without further delay?" (*disclose*). Responses to all dependent variables were recorded on a 7-point scale labelled "Not at all" (1) and "Very likely" (7) or the relevant equivalents.

Finally, demographic information including age, sex, rank, level of security clearance, and years of ADF service was collected. Participants were then thanked for their time and invited to provide comments.

Results

Missing data

There were two cases of missing data. In each case, missing data was substituted with the median of the relevant variable for the sample as a whole.

Data reduction

The two items measuring perceived need-to-know were highly inter-correlated and were therefore combined to create a single scale (α=.82).

Manipulation check

The measure of perceived controllability was positively skewed in each of the four conditions. Specifically, around half (n=49) the respondents indicated that they felt they would have no control over how the requestor used the information at all (M = 1) with the remainder (n=36) indicating that they felt they could exert some degree of control in this regard (M = 3.06). Thus, the perceived control item was split into two conditions in which the potential discloser perceived they had either no control over how the requester used the information (*absent*) or had some degree of control in this respect (*present*).

Analysis of variance

Scores on all dependent variables were submitted to a 2 (perceived control: absent/present) x 2 (requester's Service) analysis of variance. Means, standard deviations, and F-values are presented in Table 8.6.

We found support for H1 in that results indicated a main effect for perceived control on each of the dependent measures assessing the extent to which participants viewed the disclosure situation as risky. Compared to those who felt they had no control over how the requester might use the information, those who felt they had some control perceived disclosing without delay to present less risk to the image of their Service (Ms=4.80; 3.99; η^2 = 0.04) and less risk to their personal reputation

(*M*s=5.01; 3.59; $\eta^2 = 0.11$). Further, when participants perceived themselves to have some degree of control over how the requester would use the information, they were more confident that the requester would manage any risk to their Service (*M*=4.61) and that the final report would treat their Service fairly (*M*=4.48) than when participants saw themselves as having no control over how the information would be used (*M*s=2.54; 2.53; $\eta^2 = 0.35$, 0.33 respectively).

We also found support for H2. Compared to participants who felt they had no control over how the information would be used, those who felt they could exercise some control in this respect perceived the requester as having a greater need to know the information (*M*s=3.64; 4.96; $\eta^2 = 0.13$) and were more likely to disclose without delay (*M*s=2.31; 3.97; $\eta^2 = 0.16$).

Only very marginal support was evident for H3. In this case, there was a main effect for requester's Service on a single dependent measure, this being the extent to which participants believed the requester would manage any risks to the image of their Service. Specifically, participants rated requesters from their own Service as more likely to manage such risks than those from another Service (*M*=3.88; 3.27, respectively; $\eta^2 = 0.05$). There was no interaction between perceived control and the requester's Service whereby high levels of the former attenuated Service-loyal disclosure outcomes. Hence no support was not found for H4.

Mediational analysis

In order to examine the potential mediating role of need-to-know in the relationship between perceived control and the intention to disclose without delay, a mediational analysis was conducted (Figure 8.1). Consistent with the results above, the requester's Service was not a significant predictor of either need-to-know or intention to disclose without delay. However, while perceived control was a significant predictor of disclosing without delay, the strength of this association was reduced when need-to-know was entered into the model.

Table 8.6

Means, standard deviations, and F-values for key dependent measures as a function of perceived controllability and requester's Service.

Perceived control	Absent		Present		*F*-values		
Requester's service	Own	Other	Own	Other	PC	RS	PC x RS
Item (if scale no. items)							
Image	4.67 (2.32)	4.93 (1.88)	3.73 (1.88)	4.26 (1.79)	3.93*	0.96	0.12
Reputation	4.75 (2.34)	5.26 (1.82)	3.18 (1.86)	4.00 (1.98)	11.70**	2.58	0.14
Manage	2.63 (1.53)	2.44 (1.42)	5.14 (1.21)	4.09 (1.59)	49.14***	4.31*	2.15
Fairness	2.54 (1.47)	2.52 (1.58)	4.91 (1.19)	4.04 (1.36)	44.83***	2.33	2.10
Need-to-know (2)	3.44 (1.62)	3.69 (1.69)	4.64 (1.47)	4.80 (1.38)	13.27***	0.43	0.16
Disclose	2.25 (1.80)	2.30 (1.77)	4.27 (2.05)	3.48 (1.83)	17.71***	0.97	1.29

Note: PC = Perceived control; RS = Requester's service;

*$p < .05$; ** $p < .01$; ***$p < .001$; *Df (1, 81).*

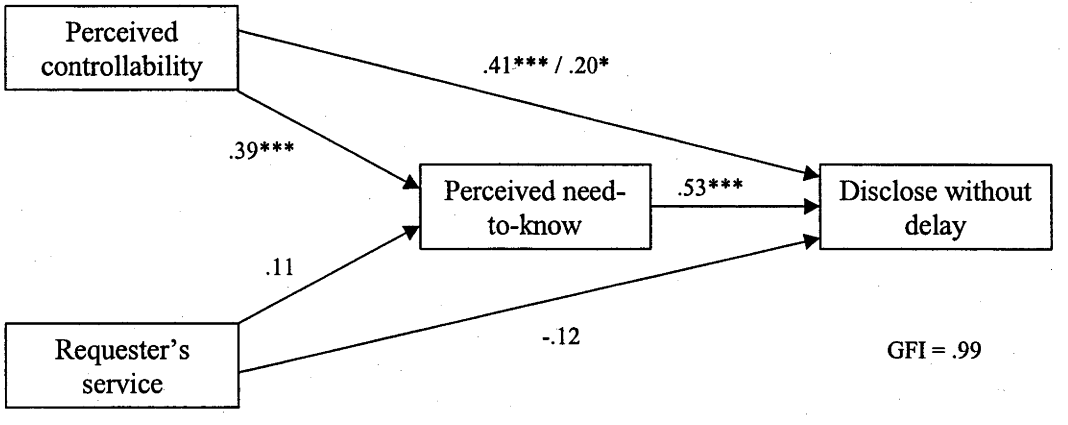


Figure 8.1 Partial mediation of the impact of perceived controllability on intentions to disclose without delay by perceived need to know.

*p<.05; ***p<.001

Qualitative data

In the context of the other studies conducted in the thesis, one of the most interesting results of Study 5 was the general absence of any Service-loyalty effect. Specifically, the findings in this study indicated that an effect for the requester's Service was only observed on one dependent measure, in this case, the extent to which the requester was expected to manage any risk to the image of the participant's Service. Here, participants expected less risk in this respect when the requester was from their own Service rather than from another Service. This isolated Service-loyalty effect stands in sharp contrast to the results reported in Study 4 where intra-Service disclosure was considered by participants in that study to be far less risky than inter-Service disclosure on all of the dependent measures. It also stands in contrast to the results of Studies 2 and 3 where the requester's Service was found have a significant effect on a number of key variables including the extent to which the requester was deemed to have a need to know the information and the likelihood that participants would disclose to the requester without further delay.

This variation in the extent to which Service boundaries affect the perceptions and prospective disclosure intentions of participants calls into question the idea that Service-loyalty is likely to be an inevitable part of the disclosure environment of the ADF. Indeed, and apart from the findings of Study 4, it must be remembered that the Service-loyalty effects reported throughout the thesis have often yielded only small effect sizes and been qualified by interactions with other variables. For example, participants in Study 1 were only prepared to favour their own Service over another Service when they could be assured that their breach would not lead to being formally punished. Given this, it was deemed appropriate to flesh out the variation in Service-loyalty across all thesis studies with qualitative data collected by way of interviews and invited comments made on experimental questionnaires[16].

One of the most common themes expressed in this data was that personal experience outside of one's Service environment was likely to reduce the extent to which Service boundaries were perceived as psychological barriers to the disclosure

---

[16]. For data collected by way of interviews, those interviewees were not actual participants in any of the studies reported in this thesis.

of classified information and communication more generally. This theme is well illustrated in the following response of one participant:

> Personally, I find that in my last 3 years of employment, which has been in a very high level Joint Headquarters has fundamentally changed my view on these issues. More than 3 years ago, I would have been swayed towards decisions which protected my parent Service. However, the last three years where I have been intimately involved in the planning and execution of several ADF operations involving the forces of all 3 Services, has given me a different perspective. I now believe that protection of the ADF's position as a whole is more important than that of the individual Service. In fact, I am now somewhat dismayed by the attitude of individual Services who apparently vehemently defend their positions to the detriment of the ADF (and Australia) as a whole, and the senior management of these Services are the worst offenders! (Study 1, Participant 42).

It is also expressed in the words of an RAAF officer interviewed during the course of the research. In this case, the officer had spend a number of years in a Joint area and had recently returned to AFHQ. According to this officer:

> The joint culture and the single service culture that I've experienced are very different. I was surprised and I guess disappointed, having had four years out of the headquarters, to come back into it - that's the RAAF headquarters, to see just how much - how many decisions are made here based on stories and anecdote and not on analysis...In the Joint domain, what's different there I suppose from my experience where I was is that...maybe because we don't have the stories that are common across Army, Navy and Air Force, we're forced to build a common set of metaphors and a common set of understandings...In the context of building Joint capabilities like command support systems and communications systems you're forced to analysis because you've got no other way of building a common language that then bring a whole bunch of stakeholders to the one table. (Interviewee 1)

In some cases, participants simply expressed individual attitudes consistent with this broader theme of cooperation, irrespective of whether they had served in areas of the ADF outside of their particular Service. For example, one participant in Study 1 remarked:

> My loyalty is to the ADF personnel, the ADF, and the Australian people, not to "projects" or "capability studies" which come and go. If this exercise does not show this then it is misleading. (Study 1, Participant 76)

A similar attitude was voiced by a participant in the final study:

> Capability deficiencies need to be managed as an ADF problem not just a single Service issue and therefore if an Army problem, "we" should be looking to improve this, not "tribal infighting". (Study 5, Participant 22)

A further theme derived from the qualitative data was that problematic non-disclosure of classified information was more likely to follow the contours of Service boundaries at higher strategic levels of the ADF than at lower tactical levels. More specifically, it was the strategic levels of the organization that were seen to be the most prone to experience severe inter-Service rivalries and jealousies capable of inappropriately affecting the flow of classified information. In contrast, problematic non-disclosure of such information was regarded as less likely amongst those conducting actual military operations, as implied by the following participant:

> I hope your study discriminated between inter-Service politics (i.e., Canberra) and the conduct of operations. (Study 3, Participant 194)

and another:

> Information flow between different colour uniforms isn't the problem...The political machinations of what the recipient does with the information is *the problem*. Different Services compete for the same bucket of money so what can be embarrassing for one Service could profit another...I have not come across peers from different Services deliberately screwing each other over, but their bosses have. (Study 3, Participant 119; emphasis in original).

This idea that the prevailing military/defence context influences the extent to which Service boundaries are likely to constitute disclosure barriers was also examined in interviews with a number of serving ADF personnel. In one interview an officer of the ARA was questioned as to if and why strategic areas of the ADF were more likely to suffer problematic non-disclosure of classified information than tactical or operational levels, to which they replied:

> ...the trouble is that at the strategic level it becomes so much more complex... because you have got so many other factors to consider. When you are talking about joint operations at a tactical and operational level, for example, finance is not a consideration, if you know what I mean. Money is not really a factor in tactical and operational planning in a military domain. At a strategic level money is everything. (Interviewee 2)

These sentiments were echoed in the words of the RAAF officer interviewed. When asked to describe the relationship between the culture of the strategic-level RAAF Headquarters and disclosure outcomes, this officer argued that senior officers at strategic levels of the RAAF like to think in terms of...

> ...their tribal roots, if you like. And what's pretty interesting about that is that most of them, I sense, are very comfortable doing that - not too many are uncomfortable...and that when they're there, the disclosure is okay in terms of the RAAF, within the tribe. But there is very much an expectation that some stuff will be held within that group and not be shared with the others as they're seen as potential adversaries, predators in terms of money, or competitors in terms of money. So at that point that value of the RAAF and its integrity into the future as an organisation is the paramount value, more important than the defence of Australia or building a balanced defence organisation, which actually might mean de-investing in RAAF and investing more in Army and Navy... that's not seen as an option. (Interviewee 1).

It is argued that this qualitative data collected by way of interviews and experimental questionnaires provides some insight into the complexities associated with whether Service boundaries will surface as problematic features in the terms of the disclosure of classified information in the ADF. From this data, it is possible to discern a number of complex and interrelated themes and issues that are likely to play a role in this respect. Professional experience beyond the boundaries of one's Service, one's attitude toward the ADF, and whether one is located with an operational- or strategic-level environment are all likely to be implicated to some extent in the response of participants to the issues raised in the empirical studies conducted through this thesis.

Discussion

Our aim in Study 5 was to provide a direct test of the guardedness hypothesis. As outlined above, this hypothesis holds that problematic non-disclosure of Service-sensitive classified information represents a cautiousness or circumspection aroused by perceived uncertainty as to whether the requester will use the information in a way that harms the potential discloser's Service. In Study 5, our specific goal was to investigate whether uncertainty of this kind was causally related to three variables: the perceived riskiness of the disclosure situation, the need to know of the requester, and likelihood of prospective disclosure without further delay. Extending work that has been conducted in the field or organizational decision-making under risk (e.g., Forlani, 2002), we varied the level of uncertainty surrounding the requester's use of the information by manipulating the extent to which participants felt they could control the requester in this respect.

The results of Study 5 provided strong support for the guardedness hypothesis. When participants perceived they had some degree of control over how the requester might use the information requested, they judged the disclosure situation to be less risky compared to when they perceived themselves to have no such control. This support for H1 was observed on each of the variables that assessed the amount of risk perceived to be present in the disclosure situation. Specifically, a degree of perceived control led participants to perceive there to be less risk to the image of their Service, less risk to their own personal reputation, a greater likelihood that the requester would manage any risk, and a greater likelihood that the information would be used in a way that treated the participant's Service fairly. Results here also provided strong support for H2. That is, when participants perceived they had some degree of control over how the requester might use the information requested, they attributed to a greater need to know to the requester and were more likely to disclose the information without delay than when they perceived themselves to have no such control.

These findings are consistent with and extend those of organizational decision-making under risk reported in previous literature. Generally speaking, past studies have shown that organizational decision-makers (managers, investors, and the like) are more likely to choose the risky options when they believe they can influence to

some extent, the outcomes of these decisions, that is when they have a degree of 'outcome control' (Forlani, 2002; March & Shapira, 1987; Shapira, 1995). Our findings also reflect prior arguments made by organizational sociologists concerning organizational secrecy. By focusing on issues of perceived risk, Study 5 also reflects many of the ideas presented in the decision-theoretic literature concerning risky choice, such as expected utility theory (Savage, 1954; von Neumann & Morgenstern, 1944), regret theory (Bell, 1982; Loomes & Sugden, 1982) and prospect theory (Kahneman & Tversky, 1979). In this theoretical vein, our manipulation of perceived control could be seen as a manipulation of *outcome variability*. That is, when a sense of perceived control was lacking, the possible outcomes of disclosure were more variable, and hence opened up the possibility of negative outcomes. We can see support for this idea in the responses of participants about the degree to which the disclosure situation involved risk. When participants believed they had no control over the use of the information, disclosing without delay was perceived to pose a greater risk, to both the image of one's Service and to one's personal reputation, than when one believed that they could influence the way in which the information was used. Thus, the present findings extend the applicability of the fundamental ideas of theories of decision-making under risk further into the organizational domain, but this time with respect to disclosure behaviour, rather than purely economic decisions.

The results of Study 5 yielded only very limited evidence of a Service-loyalty effect and, in doing so, provided only marginal support for H3. In this case, we observed that personnel were more confident that risks to their Service would be managed when the requester was also from this Service than from another Service. As was discussed above, this limited evidence of a Service-loyalty effect stands in contrast to the relatively large impact of a Service boundary that was suggested by the findings in Study 4. In order to explain the marked variability in which Service-loyal disclosure outcomes have emerged throughout the course of the thesis, it is necessary to appreciate the complexity of factors outside of our experimental control that contribute to either increasing or decreasing the salience of Service boundaries in shaping disclosure outcomes. In a review of the qualitative data collected by way of interviews and study questionnaires, it is apparent that a number of complex and interrelated factors are important in this respect. These include (but are arguably not limited to) the nature of personnel's experiences outside of their single-Service

environment, their attitudes towards the ADF, and the nature of the prevailing defence context in which these studies have been conducted.

From the findings of Study 5, we can provide a tentative explanation as to why the Service-loyalty effect was limited to this measure alone that is consistent with the themes derived from the interview data. Specifically, the majority of the participants who took part in Study 5 were drawn from Headquarters Northern Command (HQNORCOM), a Joint operational-level organization whose role is to conduct Joint operations in the northwest of Australia. Unlike the sample from DJFHQ in which participants for Study 4 were drawn, HQNORCOM is comprised of somewhat equal numbers of RAN, RAAF, and ARA personnel. Furthermore, HQNORCOM is responsible for the conduct of ADF operations, primarily the coastal and aerial surveillance of Australia's maritime exclusion zone (e.g., Operation RELEX). As with all ADF operations, success here depends upon the close cooperation of RAAF and RAN capabilities and personnel. As a result, Service-loyalty could be expected to be both incommensurate with the culture and the functional responsibility of the Headquarters.

General conclusions

The guardedness hypothesis of problematic non-disclosure holds that the phenomenon is a protective response to risk. In the context of this thesis, this hypothesis suggests that ADF personnel will be motivated to withhold classified information that is sensitive to the interests of their Service because of fears as to how the potential recipient or those 'further down the line' may use to the information. Thus, the hypothesis constitutes an alternative to that in which Service identity is considered to be a central and driving element of problematic non-disclosure. According to the guardedness hypothesis, the Services of the ADF are only likely to be part of a non-disclosure problem to the extent that the potential discloser perceives those from other Services as more likely to be malicious, careless or ignorant of the sensitivities associated with the disclosure of this type of information.

In this chapter, we conducted two tests of the guardedness hypothesis. In the first, we sought merely to demonstrate that ADF personnel perceive the disclosure of

classified information, both within and across their Service boundaries, to be associated with various classes of risk, such as uncertainty as to how the disclosed information might be used. Not only did we find support for this idea, we also demonstrated that the extent to which personnel feel confident toward such risks is related to their overall level of confidence in determining the need to know of others. In the second study (Study 5) we tested the guardedness hypothesis more directly, seeking causal rather than correlational findings. Based on a manipulation of the extent to which participants felt they could control the actions of the potential recipient post-disclosure, it was possible to systematically vary the extent to which participants perceived the disclosure situation as risky, the extent to which they attributed to the requester a need to know, and the extent to which they were likely to disclose to the requester without delay. In short, the findings of Study 5 provided strong support for the guardedness hypothesis as a psychological account of problematic non-disclosure of Service-sensitive classified information.

In providing this support, the results of Study 5 proved particularly valuable in a second respect. Specifically, we can now conclude with some certainty that Service-loyalty is not an inherent or inevitable factor in the disclosure environment of the ADF. In providing only a very limited Service-loyalty effect, the findings of Study 5 direct us to an appreciation of the complexity surrounding the extent to which Service boundaries are likely to impact classified disclosure outcomes. Past experiences, attitudes to the ADF, location in the ADF, and the nature of the prevailing military environment each emerged through qualitative data collected by way of interviews and questionnaires as a potentially important factor in this respect. These findings, together with those of the foregoing chapters and their implications for understanding problematic non-disclosure of classified information in the ADF are revisited in Chapter 9, the final chapter of this thesis.

CHAPTER 9

SUMMARY & CONCLUSIONS

Introduction

At the beginning of the thesis we asked: why might people who share a common organizational purpose fail to disclose valuable knowledge and information to each other when non-disclosure could have negative, even disastrous outcomes? Clearly, this question has become increasingly significant in the post-September 11 environment and in the wake of other major events that have issues of 'who knew what?' and 'why wasn't it passed on?' at their core. In this thesis, we have attempted to provide an answer to the question as it relates to the non-disclosure of classified (i.e., officially secret) information in the ADF context. Our focus on this type of information and this organization is not due to any prior acknowledgement that the flow of classified information throughout the ADF is beset with problems (though at times this has been suggested; see Marr & Wilkinson, 2003) but for two interrelated reasons. The first is that problematic non-disclosure of classified information amongst ADF personnel could have disastrous consequences for the organization including the loss of national security and conceivably the loss of life. The second reason is that there is an assumption that official rules will ensure that any non-disclosure of classified information amongst ADF personnel is always 'appropriate' non-disclosure and, as has been argued above, this assumption cannot be maintained.

These first steps toward a psychology of problematic non-disclosure in the ADF have been guided by more than one theoretical framework. We have drawn on research conducted not only across different areas of psychology but also on theory and research conducted outside of this discipline. On the basis of our findings, it is argued that problematic non-disclosure of classified information, in this case that sensitive to Service interests, is a protective response to perceived risk concerning how the information will be used if disclosed. Specifically, problematic non-disclosure of the kind investigated here represents a form of guardedness that manifests as a reluctance to attribute to the potential recipient a need to know such information and an unwillingness to disclose the information to them without further

delay. In this the final chapter, a summary of the thesis is presented and the implications of our findings for both organizational practice in the ADF and the literatures reviewed are outlined. Following this, some limitations of the research program are discussed as are directions for future research. The chapter concludes with a final comment about the broader implications of the thesis.

Summary

Where Chapter 1 discussed the background to the research problem and provided an overview of the thesis chapters, Chapter 2 set the scene for a psychological analysis of problematic non-disclosure of classified information in the ADF context. The official rules governing access to classified information provided the backdrop to this process and it was argued that these rules constitute a formal model from which we derive a commonsense view of disclosure outcomes. Specifically, the formal model suggests that classified information comes to be known by those who have a 'need to know' if, and only if they also possess an adequate-level security clearance. We argued that while the formal model is necessary and may suffice as an explanatory framework when there is consensus about the appropriateness of disclosure outcomes, it is not sufficient as an explanatory framework when this is not the case. More specifically, it fails to explain the when and why of problematic non-disclosure of classified information. It was argued that any such explanation must recognise that the disclosure of classified information and more specifically, the determination of 'need to know' involves psychological processes of judgment and attribution. Therefore, the focus of the thesis shifted toward gaining an insight into the contribution that psychology has made with respect to understanding the factors affecting disclosure behaviour.

In Chapter 3, this contribution was reviewed. Disclosure and non-disclosure were found to be central to a number of phenomena that have attracted the attention of researchers interested in issues of psychological process. The bulk of this work has been devoted to self-disclosure (Hendrick, 1987; Jourard, 1971) where the interplay of risk and trust is a core theme. From self-disclosure, we turned to the confidentiality literature which addressed the issue of problematic non-disclosure directly because of the potential for non-disclosure to have negative (i.e., *Tarasoff*-type) consequences.

In this area, the potential discloser was cast as a decision-maker weighing up the expected costs and benefits of disclosing and of withholding information from an ever-increasing number of parties seeing themselves as having a legitimate need to know. This idea was also evident in discussions about the psychology of whistle-blowing (e.g., Dozier & Miceli, 1985; Gundlach et al., 2003). Yet, an additional insight was provided here in that the discloser (i.e., the whistle-blower) was viewed as someone behaving in a *prosocial* way, that is, in the interest of others (Brief & Motowildo, 1986; Miceli et al., 1991; Street, 1995). The idea that affiliation underpins one's disclosure intentions was taken a step further in a review of secrecy as it relates to families, organizations and secret societies (e.g., Ericson, 1989; Vangelisti & Caughlin, 1987). On the basis of this review we distilled two 'master factors' thought likely to be implicated in the disclosure of classified information in the ADF context - *risk* and *group affiliation.*

The empirical work began in Chapter 4 where the effects of risk and group affiliation on prospective disclosure intentions was examined in two studies. Here, we followed the path laid by those examining problematic non-disclosure in the area of confidentiality (e.g., Knowles & McMahon, 1995; Lindenthal et al., 1984) by investigating whether ADF personnel were prepared to disclose against the mandate of official rules (i.e., to breach national security) in order to avoid negative outcomes and if so, when and for whom. To that end, a pilot study was conducted involving a sample of DSTO scientists bound by the same rules governing access to classified information as their ADF counterparts. These participants were given a set of disclosure dilemmas, in which prospective disclosure would breach national security policy or a less formal condition of entrustment, and non-disclosure would negatively affect either a colleague, a division, or DSTO at large. While prepared to prospectively breach the less formal conditions of entrustment, particularly when they were affiliated with the element harmed by non-disclosure, these participants were largely unprepared to prospectively breach national security via the unofficial disclosure of classified information under *any* conditions.

However, different results were obtained in the main study of Chapter 4 (Study 1) which involved a larger sample of ADF personnel. In Study 1, we again presented participants with various entrustment scenarios including one in which they

were hypothetically entrusted with classified information. As with the pilot study, a decision to prospectively disclose would constitute a breach of national security policy (or a less formal condition of entrustment) whereas a decision to withhold the information would allow harm to befall a colleague, a Service, or the ADF at large. The results showed that these participants grew increasingly willing to prospectively disclose the classified information as the consequences of non-disclosure grew progressively more severe. Further, the rate of prospective disclosure increased significantly when participants expected to evade formal punishment for any such breach. While these results supported the idea that risk moderates problematic non-disclosure, the most interesting results were arguably related to participants' Service affiliation. Specifically, we found that participants were more willing to prospectively breach national security when non-disclosure threatened to harm their own Service compared to another Service, albeit when they expected their breach to go unpunished. This suggested that problematic non-disclosure of classified information in the ADF may be likely to surface around the organization's Service boundaries. As a result of these findings, our focus shifted in Chapter 5 toward the social identity perspective as a potential explanatory framework for understanding the psychology of problematic non-disclosure of classified information in the ADF.

In Chapter 5, the social identity perspective, comprising the arguments of both social identity theory (Tajfel & Turner, 1979) and self-categorization theory (Turner, 1985; Turner et al., 1987) was reviewed. Underlying the perspective as a whole is the idea that people perceive and respond to the world in a qualitatively different way when they define themselves as members of social groups than as unique individuals (Turner, 1999; Turner & Haslam, 2001). Based on work conducted in the tradition of social identity theory (e.g., Tajfel et al., 1971), the perspective holds that just as individuals wish to evaluate themselves positively as individuals (Festinger, 1954), so too do they seek positive self-evaluation as group members (Tajfel, 1978; Tajfel & Turner, 1979). Moreover, the establishment, maintenance or enhancement of a positive social identity is thought to involve intergroup comparisons in which one's ingroup is positively distinct from relevant outgroups (Tajfel & Turner, 1979; see also Turner, 1975). Additionally, based on work in the tradition of self-categorization theory, the perspective maintains that social identities are categorizations of the self (Onorato & Turner, 2002, 2001; Turner & Onorato, 1999). It is said that when a self-

category becomes psychologically salient, a process of depersonalization occurs whereby other ingroup members are perceived to be categorically interchangeable with the self (Turner et al., 1987). According to the perspective, depersonalization aligns the goals and interests of group members and makes collective behaviour possible (Turner et al., 1987).

Two preliminary hypotheses of problematic non-disclosure were formulated from these ideas. First, it was argued that problematic non-disclosure of classified information between the Services is driven by the need to preserve a valued social (in this case, Service) identity. Second, it was held that problematic non-disclosure of this type arises when potential discloser perceives the potential recipient as a member of a salient outgroup. In support of the first of these ideas, we reviewed work conducted both within and outside of the social identity tradition suggesting that in order to establish or preserve a sense of group affiliation, people vary not only what they communicate but *to whom* they communicate (e.g., Suzuki, 1998). Attention was also focused on those groups and societies such as the Intelligence Community in which those who claim they belong are expected to keep certain knowledge and information concealed from outsiders (Bellman, 1981; Kaiser, 1980; Simmel, 1906; see also United States House Committee, 2002). In support of the second of these ideas, a brief review was made of work within the social identity tradition that demonstrates that people are less willing to cooperate with outgroup members (e.g., Ellemers, van Rijswijk et al., 1998; Tyler, 1999; Tyler & Blader, 2000, 2001; Wit & Wilke, 1992), as they are more likely to perceive outgroup members as less trustworthy (Allen & Wilder, 1975; Brewer, 1981; Kramer, 2001; Yamagishi et al, 2003).

These hypotheses were tested in Studies 2 and 3 respectively which were presented in Chapter 6. Here, our general approach shifted somewhat. Rather than situating these hypotheses within the context of breaches of national security and the like, we examined their validity by examining ADF personnel's perceptions of and responses to routine requests for classified information. Our approach also shifted in terms of specifying the kind of classified information of concern. In line with work reviewed in Chapter 5, our attention turned to classified information relating to sensitive issues about the potential discloser's Service, in this case their Service's

capability. Finally, we sought greater specification as to the form that non-disclosure might take. For example, would non-disclosure manifest as delayed decisions, passing the request up the chain of command, or verifying the potential recipient's access credentials?

The first preliminary hypothesis was set in the context of the Jointness ideology. There was good reason for doing this. Since Jointness emerged at the end of World War II, there has been continual debate in Australia and overseas about the extent to which a nation's armed forces should be 'Joint' (e.g., Ankersen, 1998; Codner, 1998, Wilkerson, 1997). A fundamental theme running through this debate concerns the potential for Jointness to undermine the distinctiveness of single-Service customs, traditions, and identity (e.g., Trainor, 1993-4). Thus, a manipulation of the Jointness ideology (i.e., a threat to Service distinctiveness or not) and the requester's Service (i.e., own or other) was used to examine not only the independent effects of each factor, but also whether Service-loyal disclosure outcomes would be accentuated when Service distinctiveness was threatened and attenuated when it was preserved. The results of Study 2 provided little support for these predictions. Jointness did not emerge as a clear threat to Service distinctiveness and identity. Yet, the results did indicate significant interactions between the requester's Service and the likelihood that certain courses of action would be taken. Compared to an own-Service requester, participants trusted an other-Service requester less, were less likely to disclose to an other-Service requester immediately, were more likely to delay responding to an other-Service requester, and were more likely to pass responsibility for dealing with an other-Service requester up the chain-of-command.

The second preliminary hypothesis was set in the context of a Service-relevant opinion-based group (see McGarty & Bliuc, 2004). Here, we established an opinion based on a respect for the potential discloser's Service, that is, being a 'supporter' of this particular Service, as the criteria for shared group membership. In other words, we created a new self-category for the potential discloser about their Service that could include both own and other-Service requesters as 'supporters' of this Service. Thus, a manipulation of both the requester's opinion (i.e., supporter or non-supporter) and the requester's Service (i.e., own or other) was used to examine not only the independent effects of each of these factors but also whether Service-loyal disclosure

outcomes would be accentuated when the potential recipient was an outgroup member (i.e., a non-supporter) and attenuated when they were an ingroup member (i.e., a supporter). Results of Study 3 showed that the manipulation of identity had a number of positive effects on participants' perceptions about the requester, regardless of the requester's Service. That is, when the requester was an ingroup member, participants perceived them to be more trustworthy, and indicated that they would more willing to respect their concerns 'if the tables were turned' than when the requester was an outgroup member. Furthermore, ingroup requesters were also attributed a greater need to know the information than outgroup requesters. However, participants were no more willing to disclose the information to an ingroup requester than they were to an outgroup requester. Additionally, and like in Study 2, the manipulation of the requester's Service had a number of effects on key measures. Most importantly, compared to own-Service requesters, those belonging to another Service were perceived by participants to have less of a need to know and were less likely to be disclosed the information without further delay. These findings shifted the focus of the thesis in Chapter 7 toward examining more fully how the second 'master factor', of perceived risk, shapes disclosure outcomes generally and whether it plays a role in the Service-loyal findings observed in Studies 2 and 3.

In Chapter 7, we reviewed three theories of decision-making under risk that have been influential within the broader decision-theoretic literature at some time. These were subjective expected utility theory (Savage, 1954; von Neumann & Morgenstern, 1944), prospect theory (Kahneman & Tversky, 1979), and regret theory (Bell, 1982; Loomes & Sugden, 1982). While these theories are rarely mentioned in research investigating how people make risky decisions in organizational contexts, their core hypotheses are reflected in many of the findings of organizational research (see March & Shapira, 1987; Shapira, 1995). Despite this, non-disclosure has not been a dependent variable of interest in this literature. Instead, the focus has been on management and investment decisions (e.g., Forlani & Mullins, 2000). In order gain an insight into the relationship between risk and non-disclosure, we needed to step outside the psychological literature and turn to the sociological literature concerning organizational secrecy.

Consistent with the psychological literature examining the relationship between perceived risk and self-disclosure (Kelly, 2001; Petronio, 1999), risk is also considered to be a major determinant of disclosure outcomes in sociological analyses of organizational secrecy (Coser, 1963; B. H. Erickson, 1981; Erickson, 1979; Lowry, 1972; Shils, 1956; Wilsnack, 1980). In this work, risk is viewed as a factor shaping the organization from either the outside or from within. In the former, risk is seen as justifying the need for organizational secrecy (Bok, 1984; Erickson, 1979). In the latter however, risk is viewed as bringing about dysfunctional disclosure outcomes within the organization (see Lowry, 1972; Shils, 1956). Here, other members of the organization may be perceived to be malicious in their intent, or thought likely to be careless with the information or ignorant of its sensitivities (Erickson, 1979). A general hypothesis of problematic non-disclosure of classified information in the ADF was formulated along these lines. Specifically, we concluded Chapter 7 by arguing that uncertainty as to how classified information may be used leads to the potential discloser to be *guarded* in the attitudes and behaviours toward the potential recipient, particularly when the latter belongs to another Service.

In Chapter 8, the guardedness hypothesis was tested. In Study 4, the aim was twofold. First, we sought to validate the idea that disclosure of classified information within and across Service boundaries is associated with various risks. Second, we wished to show that the extent to which the potential discloser lacked confidence about these risks was related to their level of confidence about determining need to know. To that end, we asked a sample of ADF personnel to rate how confident they were about various issues including their ability to predict how classified information they disclose might be used and that the recipients of the information would recognise and manage any risks to their Service. We also asked them to rate how confident they were about determining the need to know of potential recipients. In line with our expectations, results indicated that participants were more confident in these respects when disclosing would take place within their Service rather than across Service boundaries, not that this meant intra-Service disclosure was perceived to be risk-free. Moreover, findings showed that as participants lost confidence with respect to being able to determine how the disclosed information might be used and whether the potential recipient would recognise and manage any risks, they also lost confidence about their ability to determine a potential recipient's need to know.

On the basis of these findings, we tested the guardedness hypothesis more directly in Study 5. Specifically, we sought to determine whether perceived risk relating to how the potential recipient might use classified information was causally related to perceived need to know and prospective disclosure intentions. The study was conducted not only against the backdrop of sociological work arguing that this class of risk transforms the relations between an organization's members but also against work in organizational decision-making suggesting that guardedness may be moderated by the decision-maker's belief that they retain some form of control over decision outcomes (Forlani, 2002; March & Shapira, 1987; Shapira, 1995). That is, when the decision-maker believes they can control the outcomes of their decision, they will be more willing to make what otherwise appear to be risky decisions. Thus, a manipulation of perceived control as to how disclosed information might be used (low or high) and requester's Service (own or other) was used to examine not only the independent effects of each factor, but whether Service-loyal disclosure outcomes were accentuated when perceived control was low and attenuated when it was high.

The findings showed that the manipulation of perceived control had an effect on all dependent variables. Specifically, when compared to those who perceived themselves to have no control whatsoever over how the disclosed information might be used, participants who possessed some control viewed the disclosure scenario as far less risky, perceived the requester as having a greater need to know, and were far more likely to prospectively disclose the information without further delay. Further, perceived need to know was shown to partially mediate the extent to which perceived control influenced participants' intentions to prospectively disclose without delay. The findings also showed that the requester's Service only had an impact on only one dependent measure, that being the extent to which participants believed that the requester would manage any risks to the image of their Service. Moreover, the requester's Service did not interact with perceived control over how the information would be used by the potential requester. In light of these latter results, we concluded Chapter 8 by drawing on qualitative data to help explain the variance in Service-loyal perceptions and intentions observed over the course of the research program. That data underscored the complexities associated with the disclosure of classified information within and across the Services of the ADF, drawing attention to a number

of factors outside of experimental control, such as one's past training and experience and the nature of prevailing defence context.

Integration and implications

Provided they possess an adequate-level security clearance, it is assumed that ADF personnel come to know classified information when they have a 'need to know' that information. The intent of this thesis was not to challenge this assumption as it is written here, nor to argue against the use of formal decision-making criteria to govern access to classified information. To do so would be both misguided and unhelpful since defence organizations, perhaps more than any other, rely upon a system of rules to ensure effective disclosure and non-disclosure of their most valuable information. However, what this thesis does provide is a psychological account of how ADF personnel interpret and respond to these rules. In doing so, it challenges their subtext - that an individual's need to know classified information is impartially determined to be either present or absent and that any problematic non-disclosure of classified information must be thought of as an aberrant event.

The hypotheses tested in this thesis have emphasized either one of the two factors we derived in Chapter 3 as likely to be involved in problematic non-disclosure of classified information in the ADF. The first factor was group affiliation and here, the group of interest was the potential discloser's Service. Informed by theory and research in the social identity tradition, we derived psychological hypotheses of problematic non-disclosure of classified information in the ADF in which Service identity was central. It was argued that problematic non-disclosure was likely to be a problem with or, more accurately *between* the Services of the ADF, arising from either a self-categorical gulf between the organization's army, navy and air force personnel or the defence ideology of Jointness. Yet, the studies conducted to that end made it clear that problematic non-disclosure of the form examined in this thesis is not driven by issues relating to Service identity. That is, our results indicate that it is not a form of inter-Service rivalry or 'tribalism' evoked by Jointness or created by a self-categorical gulf that exists between personnel of different Services. Indeed, we have shown that ADF personnel can perceive there to be problems with Jointness concerning the status and/or distinctiveness of their Service or perceive there to be a

self-categorical gulf between themselves and other-Service personnel, yet neither represents the process that underlies problematic non-disclosure of Service-sensitive information between them. Therefore, it would be wrong to the lay the blame for problematic non-disclosure of the form we have investigated here at the feet of the three Services.

Having said this, we have shown that overtures which make salient a shared social identity where behaviour supportive of the participant's Service is normative are likely to evoke a more cooperative orientation amongst ADF personnel. By creating such a social identity in Study 3, it was possible to increase the extent to which our participants perceived other-Service personnel as trustworthy, as being on 'the same side', and as having a need to know the information they requested. This represents a broadening of the scope of the social identity perspective as it applies to organizational practice. Specifically, the findings of Study 3 complement the continuing work of social identity theorists to improve intergroup relations in organizational contexts by understanding and seeking to manipulate the social identification processes that are involved (e.g. Eggins, Reynolds, & Haslam, 2003; Haslam et al., 2003; see also Reynolds, Turner, & Haslam, 2003). Interesting as they may be, these processes do not account for the particular phenomenon examined in this thesis. Thus, interventions that aim to improve inter-Service relations by allowing the Services to express their identities or by orienting ADF personnel toward Jointness may be effective in improving some types of inter-Service cooperation, yet our results would indicate that they will be of limited utility if the desire is to minimize or eliminate problematic non-disclosure of classified information.

The second factor thought to be involved in problematic non-disclosure of classified information in the ADF was perceived risk. We examined risk in two forms - first, as it relates to the consequences of not disclosing (the pilot study and Study 1) and second, as it relates to the consequences of disclosing (Study's 4 and 5). With respect to the latter, and informed by the sociological literature concerning organizational secrecy, we derived a psychological hypothesis which we have termed the guardedness hypothesis. This hypothesis formed an alternative to those in which Service affiliation and identity were central. Core to the guardedness hypothesis is the idea that the intentions of the potential recipient (or recipients) of classified

information can never be known with complete certainty. Specifically, it holds that problematic non-disclosure of classified information is a guarded or protective response to the risk that the potential discloser perceives with respect to how the intended recipient might use the information if disclosed. The studies conducted to test the guardedness hypothesis yielded findings that were strongly in its favour. The findings of Study 4 indicated that as personnel grew less confident with respect to the risks associated with disclosing, so too did they become less confident with determining need to know. Moreover, we were able to show in Study 5 that it was possible to vary the extent to which participants perceived the disclosure of Service-sensitive classified information to be risky by manipulating the extent to which they felt they had some control over how the recipient would use the information. In doing so, it was possible to systematically vary both participants' perception of another's need to know the information and their disclosure intentions.

On the basis of these findings, we are now in a position to offer an answer to the question that has guided this thesis. In line with the guardedness hypothesis, ADF personnel may decide not to disclose classified information about their Service, despite this being potentially problematic to the ADF as whole, because of the perceived risks associated with how the information may be used either by the recipient or further 'down the line'. Problematic non-disclosure of the type examined here is a protective response to this perceived risk, one that seeks to protect both the interests of the Service involved and of the potential discloser. Therefore, rather than represent a phenomenon where Service boundaries and identity play a central role, problematic non-disclosure of this kind represents a guardedness or circumspection amongst ADF personnel that manifests in their perceptions and behavioural intentions toward one another. In other words, it is a phenomenon not about Service identities nor inter-Service jealousies but about the information environment of the ADF. We have showed in this thesis that this information environment is not imperiled by strong views about the contributions of the Services to the ADF, nor about Jointness and the need to preserve or eliminate Service identity. Rather, problematic non-disclosure of the type examined here is a more nuanced and complex phenomenon. It is one in which the information environment of the ADF is imperiled by perceived uncertainty as to how classified information might be used once disclosed. Further, it is one in which Service boundaries may come into sharp relief or evaporate

completely depending on those involved and the prevailing organizational culture and context.

In light of the evidence for the guardedness hypothesis, a simple analysis would be one that implies there is a lack of trust between ADF personnel. That is, if there were greater trust between ADF personnel, there would be less need for the potential discloser of classified information to be guarded or protective in their orientation. Yet this simple analysis is inadequate and inaccurate. We have shown in this thesis that through a manipulation of social identity that it was to possible to systematically vary the extent to which our participants trusted the potential recipient of Service-sensitive classified information with respect to managing the information with care. Yet, it was clear that prospective disclosure intentions did not follow the contours of this trust in particular and social identity in general, as would be expected if the simple analysis were correct. The support we have obtained for the guardedness hypothesis implies more about the information environment of the ADF than the level of trust between the potential discloser and recipient at any given time. Specifically, it implies that the information environment of the ADF is one compartmentalised not only by formal security policy but by a culture of circumspection. Put another way, problematic non-disclosure reflects an information environment dominated by norms of cautiousness rather than norms of distrust. Arguably, these norms extend beyond the potential recipient of classified information as the locus of risk to encompass a more general sense of uncertainty with how information might be used by others in the immediate and not so immediate setting.

What does an information-environment compartmentalised by a culture of circumspection mean for the ADF? First, and on the basis of the findings reported in this thesis, it means that explicit attempts to de-compartmentalise the information environment (as far as is possible) that appeal to a sense of shared identity will be limited in their utility, and this has been discussed at some length above. Second, a simple analysis of the support that we have obtained for the guardedness hypothesis might imply that organizational policies and procedures must now seek to compel the potential recipient of Service-sensitive to articulate how this information is to be used. However, there are limits to the extent to which this is possible and indeed, desirable. Information can be used in a vast number of ways and therefore any formulation of

such proscriptions as to how it can and cannot be used would no doubt be difficult if not impossible. More importantly however, the modern defence organization requires flexibility in how it uses classified information and in who comes to use it. Proscriptions as to how a certain piece of sensitive classified information can be used would represent a further layer of formalization over and above that which exists already. Thus, this simple analysis of the implications of the thesis could exacerbate rather than attenuate problematic non-disclosure.

The answer we have provided to the question guiding this research has been psychological in nature. Thus, the way forward for the ADF must be one that takes account of the psychology that is central to the guardedness hypothesis. Specifically, it is one that involves changing how ADF personnel perceive the organization and its processes rather than changing the formal rules and policies that they are expected to comply with. The knowledge that ADF personnel have about the risks associated with the disclosure of classified information is key to this change. Problematic non-disclosure of the type examined here is avoidable to the extent that the potential discloser knows the needs and roles of the potential recipient(s) of the information. Put another way, in being about uncertainty, the solution to problematic non-disclosure of this type rests upon bringing about certainty. Thus, forms of cross-training of briefings in which individuals come to know how sensitive information will be used 'down the line' would appear to be an important component of any future steps taken to avoid problematic non-disclosure of classified information in the ADF. More specifically, rather than have personnel move from one area of the information environment to another, the findings of this thesis suggest that it would be particularly important to be more systematic in this process. ADF personnel must come to acquire within the context of their posting cycles a knowledge of the 'information life-cycle'. In doing so, one acquires not only a knowledge of the perceived risk at the point of disclosure but of how these risks are recognised and ultimately managed by those further along the line. This recommendation is not to say that changing the way ADF personnel perceive the organization and its processes is an easy task. However, in this case, it is a necessary one.

By way of recapitulation, three statements can be made regarding the psychology of problematic non-disclosure in the ADF context as it relates to classified

information that is sensitive to the interests of the Services. These statements refer to the key insights obtained throughout the course of this thesis. Specifically:-

1. Problematic non-disclosure of classified information in the ADF is not a form of inter-Service 'tribalism' founded on issues relating to Service identity. Therefore, neither tribalism, Jointness, nor any other phenomenon in which Service identity is likely to be central can be part of its solution.

2. Problematic non-disclosure of classified information in the ADF will not necessarily emerge around the ADF's Service boundaries. Any efforts made to break down inter-Service boundaries will not solve problematic non-disclosure of this kind.

3. Problematic non-disclosure of classified information in the ADF is a response to perceived risk and uncertainty as to how the information will be used. The key to solving or avoiding problematic non-disclosure of the kind examined here lies in increasing the knowledge of ADF personnel in this regard.

In the following sections, some limitations and considerations of the thesis are outlined, some future directions are specified, and a final comment regarding the broader implications of this thesis is made.

Limitations and considerations

Ecological validity

It is important to recognise that, despite the fact that ADF personnel were utilized as study participants, these findings were obtained within the context of scenario-based experimental manipulations. Clearly, it would have been ideal to be able to examine the extent to which these factors affected the disclosure of *actual* classified information in 'live' (or sufficiently simulated) defence environments with extraneous factors held constant. Therefore, it is possible that our manipulations may not accurately reflect actual disclosure intentions and outcomes. However, while scenario-based manipulations carry constraints relating to ecological validity, it is

through research designs of this type that psychological processes can be isolated (see Haslam & McGarty, 2003; Turner, 1981b). Indeed, we must also recognise that any study of the factors affecting the disclosure of actual classified information in relatively naturalistic setting would have invariably been influenced by extraneous factors out of our experimental control, as in arguably the case with regard to the varying degrees of Service-loyalty observed throughout the studies presented here.

Sample consistency

One of the primary considerations in being able to conduct quantitative research with serving-ADF personnel was to minimize the degree of disruption that the data gathering phases caused. In order to obtain a sufficient amount of data over the course of a number of studies, it was necessary to disperse this disruption widely by drawing participants from more than one area of the ADF. To that end, the empirical work in this thesis has involved participants from a variety of organizations. While the majority were employed at the time of their participation in 'single-Service' organizations, these have been at both the strategic (e.g., AHQ, NHQ, & AFHQ) and operational (e.g., MHQ, LHQ) levels of the ADF. Additionally, personnel were also drawn from 'tri-Service' organizations (e.g., DMO, KSS, CSS) and other organizations formally designated as 'Joint' (e.g., DJFHQ, HQNORCOM). Within studies, statistical analyses consistently showed that the type of organization from which participants were drawn had no significant effects on the various perceptions and disclosure intentions measured (nor for that matter did the particular Service participants belonged to). However, it was impossible to determine the extent to which this was the case between studies, with the sample of personnel shifting to some extent with each study. As argued above, it is possible that the varying nature of the organizational samples employed across the studies contributed the variability with which Service-loyal perceptions and disclosure intentions were evident in our results. In spite of this limitation, we have been able to observe a remarkable degree of consistency in some results across the samples employed. Furthermore, the varying nature of these samples also provides an insight into the varied cultures contained within the ADF.

The strategic defence environment

The results of all social-psychological research must be understood in terms of the prevailing social context, particularly that conducted within naturalistic settings. During the course of this research, the prevailing context as it related to military and defence affairs in Australia and internationally was shaped by a number of significant events. The most significant beyond doubt were the terrorist attacks in the United States of September 11, 2001, which ultimately drew a considerable contingent of ADF personnel from each Service into war in both Afghanistan and Iraq. However, there were also a number of other events that took place during the course of the research in which the media spotlight was focused on the ADF more directly. These included the 'Children Overboard' issue and the Bali bombings. It is possible that these events influenced how our participants responded to many of the disclosure scenarios in the studies reported in this thesis. In the wake of September 11, 2001, for example, ADF personnel may have been generally more cooperative in their perceptual and behavioural orientations toward one another than they were before the tragedy. Clearly, the nature of the research issue here rendered it impossible to control for such effects. Therefore the present findings must be viewed against the richly textured backdrop of the strategic defence environment.

Future directions

Service-loyalty

Clearly, finding that problematic non-disclosure of classified information in the ADF may also be likely to surface, to a greater or lesser extent, around the organization's Service boundaries has implications for Jointness. After many years of development and debate, Jointness and inter-Service cooperation have emerged as conceptual mainstays around which many major Australian military policies have been developed (Behm et al., 2001). A central and necessary aspect of these policies is achieving 'interoperability' between the three Services in both a technological and doctrinal sense. However, empirical findings reported throughout this thesis imply that interoperability on these dimensions may be of little value if Service boundaries are to emerge as psychologically salient barriers that denote other-Service personnel

as less trustworthy recipients of Service-sensitive classified information than own-Service personnel. It would be comforting to believe that by taking care of issues relating to both shared identity and perceived control, inter-Service boundaries would not longer constitute such a barrier. However, the results of our studies caution against making such a conclusion. It may prove worthwhile therefore, for future research to examine more closely the factors that evoke Service-loyalty in some military contexts and not others.

Beyond the ADF

Clearly, the ADF does not exist in a vacuum. Instead, the organization lies at the heart of a tightly interwoven network of organizations, each of which depends to some degree, on the others in order to make a positive contribution to the total defence effort. One of the most important interdependencies in this respect is that between military (i.e. ADF) and civilian personnel. Over the past few years, the extent to which military and civilian members of the ADO have been brought together in fully integrated organizations has increased dramatically. Furthermore, a number of the organizations upon which the ADF is dependent in a number of ways are staffed by a majority of civilian personnel. Throughout the course of this thesis, many participants expressed a concern that information-sharing between military and civilian elements of the ADO needed to be improved. Indeed, in light of the findings of this thesis, it is somewhat ironic that a participant in Study 1 wrote:

> The civilian side of Defence is one of the worst offenders when it comes to sharing information. They still staunchly protect their information in some areas because they feel that the military either do not know what they are doing, or will misuse the information. (Study 1, Participant 42)

It is desirable therefore that future research extend our current focus on inter-Service boundaries to that boundary, perceived or real, between military and civilian personnel of the ADO. There is, however, more that can be said on this point. It is the case that future ADF operations are likely to be conducted in partnership with military forces from other nations (Behm, et al., 2001). The recent ADF-led operation in East Timor, for example, involved military forces from a number of countries, many of which had little or no prior working relationship with the ADF. Given this, it

would seem appropriate to also extend the scope of the ideas examined in the thesis to include an analyses of problematic non-disclosure of classified information not only within the ADF but between this organization and those of other nations with whom it must cooperate to achieve operational success.

Final comment

A primary implication of this thesis is that we are likely to be misguided by the prevailing assumption that structural and technological improvement agendas *in and of themselves*, will enhance the exchange of classified information between ADF personnel. To date, contemporary defence science and policy in both Australia and elsewhere has succeeded in drawing attention to the need to examine new organizational structures that may be more responsive in dealing with the vast array of non-traditional functions that military organizations are required to fulfil (see Warne, Ali et al., 2003). It has succeeded to an even greater extent in terms of specifying and developing complex information technologies capable of increasing the volume, speed, and breadth with which classified information can be exchanged amongst defence personnel (see Wilson, 2004). On the basis of the work reported here, what is required now is an approach that looks beyond these factors and also resists the temptation to relegate the disclosure and non-disclosure of classified information to the status of a simple 'security matter'.

At the very beginning of the thesis, reference was made to a phenomenon known colloquially as "the Wall" (United States House Committee, 2002). Complex, politically thorny, and problematic, the Wall is as much a psychological phenomenon as it is a procedural or a physical one. In this thesis, we have taken the first steps toward teasing out the psychological 'building blocks' of the Wall as it might relate to the ADF. In doing so, work from across psychology and sociology has been brought together to formulate relevant psychological hypotheses and these have been tested with ADF personnel in the context of their daily work environments. In many respects, the teasing out of the psychological factors likely to be at work here has been a difficult process. Yet, these initial steps mark a shift in the study of contemporary defence problems and with the impeding arrival of network-centric warfare, this shift is needed now more than ever.

REFERENCES

Adams, B. D., Bryant, D. J. & Webb, R. D. G. (2001). Trust in teams: Literature Review (*Technical report CR-2001-042*). Ontario: Department of National Defence.

Aftergood, S. (2000). Secrecy is back in fashion. *Bulletin of the Atomic Scientists* 56(6): 25-30.

Allen, V. L. & Wilder, D. A. (1975). Categorization, belief similarity, and intergroup discrimination. *Journal of Personality & Social Psychology, 32*, 971-977.

Ankersen, C. P. (1998). A little bit Joint – Component commands: Seams not synergy. *Joint Force Quarterly, Spring*, 116-122.

Argyris, C. (1960). *Understanding Organizational Behavior.* The Dorsey Press, Inc. Homewood.

Ashforth, B. E. & Mael, F. (1989). Social identity theory and the organization. *Academy of Management Review, 14*, 20-39.

Australian Attorney-General's Department. (2000). *Commonwealth Protective Security Manual - 2000.* Attorney-General's Department.

Australian Department of Defence. (1979). *Australian Experience in Joint Armed Service Activities* (Historical Monograph No. 10, DRB 101). Department of Defence.

Australian Department of Defence. (1991). *Security Policy Manual 1* (SECMAN 1). Commonwealth of Australia.

Australian Department of Defence. (1998). *Defence Protective Security Manual 4* (SECMAN 4, Edition 3). Commonwealth of Australia.

Baker, General J. S. (1995). ADF command arrangements. Headquarters Australian Defence Force Minute, CDF 582/1995. Australia.

Barbour, R. A. (1994). A telling tale: AIDS workers and confidentiality. In P. Aggleton, P. Davies and G. Hart (Eds.) *AIDS: Foundations for the Future: Social Aspects of AIDS* (pp. 147-158). London: Taylor & Francis.

Beaumont, R. (1993). *Joint military operations: A short history.* Westport: Greenwood Press.

Behm, A., Allen, R., Goodyer, M., & Tregurtha, J. (2001). Joint warfare – Australia's approach to Joint operations. *Australian Defence Force Journal, 149*, 15-25.

Bell, D. E. (1982). Regret in decision-making under uncertainty. *Operations Research, 30*, 961-981.

Bellman, B.L. (1981). The paradox of secrecy. *Human Studies, 4*, 1-24.

Bennis, W.G. (1959). Leadership theory and administrative behavior: The problem of authority. *Administrative Science Quarterly, 4*, 259-301.

Berry. J. W. (1976). *Human ecology and cognitive style: Comparative studies in cultural and psychological adaptation.* New York: Sage.

Bigley, G. A. & Pearce, J. L. (1998). Straining for shared meaning in organization science: Problems of trust and distrust. *Academy of Management Review, 23*, 405-421.

Blau, P. M. & Scott, W. R. (1962). *Formal organizations: A comparative approach.* Chandler Publishing Company. San Francisco.

Bok, S. (1984). *Secrets: On the ethics of concealment and revelation.* New York: Vintage.

Bollas, C., & Sundelson, D. (1995). *The new informants: The betrayal of confidentiality in psychoanalysis and psychotherapy.* Northvale: Aronson.

Boon, S. D. & Holmes, J. G. (1991). The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. In R. A. Hinde & J. Groebel (Eds.) *Cooperation and prosocial behavior* (pp. 190-211). Cambridge: Cambridge University Press.

Boon, S. D. & Miller, R. J. (1999). Exploring the links between interpersonal trust and the reasons underlying gay and bisexual males' disclosure of their sexual orientation to their mothers. *Journal of Homosexuality, 37,* 45-68.

Boyd, R. & Richardson, P. J. (1991). Culture and cooperation. In J. J. Mansbridge (Ed.) *Beyond self-interest* (pp. 111-132). Chicago: University of Chicago Press.

Brabeck, M. (1984). Ethical characteristics of whistle-blowers. *Journal of Research in Personality, 18,* 41-53.

Branscombe, N., Ellemers, N., Spears, R., & Doosje, B. (1999). The context and content of social identity threat. In N. Ellemers, R. Spears, & B. Doosje (Eds.) *Social identity: Context, commitment, content* (pp. 68-88). Oxford: Blackwell.

Brewer, M. (1979). In-group bias in the minimal intergroup situation: A cognitive-motivational analysis. *Psychological Bulletin, 86,* 307-324.

Brewer, M. (1981). Ethnocentrism and its role in interpersonal trust. In M. B. Brewer & B. E. Collins (Eds.) *Scientific inquiry and the social sciences* (pp. 345-360). San Francisco: Jossey-Bass.

Brewer, M. (1991). The social self: On being the same and different at the same time. *Personality & Social Psychology Bulletin, 17*, 475-482.

Brewer, M. B. & Silver, M. (1978). Ingroup bias as a function of task characteristics. *European Journal of Social Psychology, 8*, 393-400.

Brief, A. P. & Motowildo, S. J. (1986). Prosocial organizational behaviors. *Academy of Management Review, 11*, 710-725.

Brown, R. (1978). Divided we fall: An analysis of relations between sections of a factory workforce. In H. Tajfel (Ed.) *Differentiation Between Social Groups* (pp. 395-429). London: Academic Press.

Brown, R. & Turner, J. C. (1981). Interpersonal and intergroup behavior. In J. C. Turner & H. Giles (Eds.) *Intergroup behavior* (pp. 33-65). Oxford: Blackwell.

Bruins, J., Ellemers, N., & de Gilder, D. (1999). Power use and differential competence as determinants of subordinates' evaluative and behavioural responses in simulated organizations. *European Journal of Social Psychology, 29*, 843-870.

Bruner, J. S. (1957). On perceptual readiness. *Psychological Review, 64*, 123-152.

CAIB. (2003). *Report: Volume 1*. Washington DC: US Government Printing Office

Cash. T. F., Stack, J. J., & Luna, G. C. (1975). Convergent and discriminant behavioral aspects of interpersonal trust. *Psychological Reports, 37*, 983-986.

Chandra Sekhar S. F. &. Anjaiah, P. (1995). Organisational communication and interpersonal trust: An evaluation of their relationships. *Psychological Studies, 40*, 28-32.

Charbonneau, A., Maheux, B., & Beland, F. (1999). Do people with HIV/AIDS disclose their HIV-positivity to dentists? *AIDS Care, 11*, 61-70.

Chattopadhyay, P. (1999). Beyond direct and symmetrical effects: The influence of demographic dissimilarity on organizational citizenship behavior. *Academy of Management Journal, 42*, 273-287.

Chattopadhyay, P. & George, E. (2001). Examining the effects of work externalization through the lens of social identity theory. *Journal of Applied Psychology, 86*, 781-788.

Codner, M. (1998). The strategic defence review: How much? How far? How joint is enough? *RUSI Journal, August*, 5-10.

Connelly, T. & Zeelenberg, M. (2002). Regret in decision making. *Current Directions in Psychological Science, 11*, 212-216.

Corcoran, K. J. (1988). The relationship of interpersonal trust to self-disclosure when confidentiality is assured. *Journal of Psychology, 122*, 193-195.

Corcoran, P. & Spencer, V. (2000). Introduction: Revealing disclosure. In P. Corcoran & V. Spencer (Eds.) *Disclosures* (pp. 1-14). Aldershot: Ashgate.

Coser, L. A. (1963). The dysfunction of military secrecy. *Social Problems, 11*, 13-22.

Costigan, R. D., Ilter, S. S. & Berman, J. J. (1998). A multi-dimensional study of trust in organizations. *Journal of Managerial Issues, 10*, 303-317.

Cropsey, S. (1993). The limits of Jointness. *Joint Force Quarterly, Summer*, 72-79.

Dahrendorf, R. (1968). *Essays in the theory of society.* Stanford: Stanford University Press.

Dasgupta, P. (1988). Trust as a commodity. In D. Gambetta (Ed.) *Trust: Making and breaking cooperative relations* (pp. 49-72). Oxford: Blackwell.

Davis, J., Schoorman, D., Mayer, R., & Tan, H. H. (2000). The trusted general manager and business unit performance: Empirical evidence of a competitive advantage. *Strategic Management Journal, 21*, 563-576.

De Cremer, D. & Van Vugt, M. (1999). Social identification effects in social dilemmas: A transformation of motives. *European Journal of Social Psychology, 29*, 871-893.

Demac, D. (1984). *Keeping America uninformed: Government secrecy in the 1980's.* New York: Pilgrim Press.

DeMatteo, D., Harrison, C., Arneson, C., Goldie, R. S., Lefebvre, A., Read, S. E. et al. (2002). Disclosing HIV/AIDS to children: The paths families take to truthtelling. *Psychology, Health & Medicine, 7*, 339-356.

Derlega, V. J., Metts, S., Petronio, S., & Margulis, S. T. (1993). *Self-disclosure.* Newbury Park: Sage.

Deutsch, M. (1958). Trust and suspicion. *Journal of Conflict Resolution, 2*, 265-279.

Doney, P. M., Cannon, J. P. & Mullen, M. R. (1998). Understanding the influence of national culture on the development of trust. *Academy of Management Review, 23*, 601-620.

Doosje, B., Ellemers, N., & Spears, R. (1995). Perceived intragroup variability as a function of group status and identification. *Journal of Experimental Social Psychology, 31*, 410-436.

Dorman, A., Smith, M. L., & Uttely, M. (1998). Jointery and combined operations in an expeditionary era. *Defense Analysis, 14*, 1-8.

Dovidio, J. F., Gaertner, S. L., Validzic, A., Matoka, K., Johnson, B., & Frazier, S. (1997). Extending the benefits of recategorization: Evaluations, self-disclosure, and helping. *Journal of Experimental Social Psychology, 33*, 401-420.

Doyle, K. (2000). The end of secrecy: U.S. national security and the imperative for openness. *World Policy Journal, 16*: 34-51.

Dozier, J.B. & Miceli, M.P. (1985). Potential predictors of whistle-blowing: A prosocial behavior perspective. *Academy of Management Review, 10*, 823-836.

Dunegan, K. J., Duchon, D., & Barton, S. L. (1992). Affect, risk, and decision-criticality: Replication and extension in a business setting. *Organizational Behavior and Human Decision Processes, 53*, 335-351.

Dunn, M. (1995). The tyranny of Jointery? The trend to tri-service organisations and the Royal Australian Navy. *Journal of the Australian Naval Institute, August/October*, 48-64.

Dutton, J. E., Dukerich, J. M., & Harquail, C. M. (1994). Organizational images and member identification. *Administrative Science Quarterly, 39*, 239-263.

Einhorn, H. J. & Hogarth, R. M. (1985). Ambiguity and uncertainty in probabilistic inference. *Psychological Review, 92*, 433-461.

Elangovan A. R. & Shapiro, D. L. (1998). Betrayal of trust in organizations. *Academy of Management Review, 23*, 547-566.

Ellemers, N. (2001). Social identity, commitment, and work behavior. In M. A. Hogg & D. J. Terry (Eds.) *Social identity processes in organizational contexts* (pp. 101-114). Philadelphia: Psychology Press.

Ellemers, N., de Gilder, D., & van den Heuvel, H. (1998). Career-oriented versus team-oriented commitment and behavior at work. *Journal of Applied Psychology, 83*, 717-730.

Ellemers, N., Spears, R., & Doosje, B. (1999). *Social identity: Context, commitment, content*. Oxford: Blackwell.

Ellemers, N., van Rijswijk, W., Bruins, J., de Gilder, D (1998). Group commitment as a moderator of attributional and behavioral responses to power use. *European Journal of Social Psychology, 28*, 555-578.

Ellsberg, D. (2003). *Secrets: A memoir of Vietnam and the Pentagon papers*. New York: Penguin.

Erickson, B. H. (1981). Secret societies and social structure. *Social Forces, 60*, 188-210.

Erickson, P. E. (1979). The role of secrecy in complex organizations: From norms of rationality to norms of distrust. *Cornell Journal of Social Relations, 14*, 121-138.

Ericson, R. V. (1989). Patrolling the facts: Secrecy and publicity in police work. *British Journal of Sociology, 40*, 205-226.

Farber, B. A. (2003). Patient self-disclosure: A review of the research. *Journal of Clinical Psychology, 59*, 589-600.

Farber, B. A. & Hall, D. (2002). Disclosure to therapists: What is and is not discussed in therapy. *Journal of Clinical Psychology, 58*, 357-370.

Fautua, D. F. (2000). The paradox of Joint culture. *Joint Force Quarterly, Autumn*, 81-86.

Festinger, L. (1954). A theory of social comparison processes. *Human Relations, 7,* 117-140.

Fiegenbaum, A. & Thomas, H. (1988). Attitudes towards risk and the risk return paradox prospect. *Academy of Management Journal, 31,* 85-106.

Fine, G. A. & Holyfield, L. (1986). Secrecy, trust and dangerous leisure: Generating group cohesion in voluntary organisations. *Social Psychological Quarterly, 59,* 22-38.

Fischhoff, B., Watson, S. R., & Hope, C. (1984). Defining risk. *Policy Sciences, 17,* 123-139.

Ford, C. A., Millstein, S. G., Halpern-Felsher, B. L., & Irwin, C. E. Jr. (1997). Influence of physician confidentiality assurances on adolescents' willingness to disclose information and seek future health care: A randomized controlled trial. *Journal of the American Medical Association, 278,* 1029-1034.

Forlani, D. (2002). Risk and rationality: The influence of decision domain and perceived outcome control on manager's high-risk decisions. *Journal of Behavioral Decision Making, 15,* 125-140.

Forlani, D. & Mullins, J. W. (2000). Perceived risks and choices in entrepreneur's new venture decisions. *Journal of Business Venturing, 15,* 305-322.

Foubert, J. D. & Sholley, B. K. (1996). Effects of gender, gender role, and individualized trust on self-disclosure. *Journal of Social Behavior & Personality, 11,* 277-288.

Gaertner, S. L., Dovidio, J. F., Anastasio, P. A., Bachman, B. A., & Rust, M. C. (1993) The common in-group identity model. In W. Stroebe & M. Hewstone (Eds.) *European review of social psychology.* vol. 4 (pp. 323-368). Oxford: Blackwell.

Gaertner, S. L., Dovidio, J. F., Banker, B. S., Houlette, M., Johnson, K. M., & McGlynn, E. A. (2000). Reducing intergroup conflict: From superordinate goals to decategorization, recategorization, and mutual differentiation. *Group Dynamics: Theory, Research and Practice, 4*, 98-114.

Gaertner, S. L., Mann, J., Murrell, A., & Dovidio, J. F. (1989). Reducing intergroup bias: The benefits of recategorization. *Journal of Personality and Social Psychology, 57*, 239-249.

Galnoor, I. (1975). Government secrecy: Exchanges, intermediaries, and middlemen. *Public Administration Review, 35*, 32-42.

Gellman, R. M. (1986). Divided loyalties: A physician's responsibilities in the information age. *Social Science & Medicine, 23*, 817-826.

Goffman, E. (1958). *The presentation of self in everyday life*. Edinburgh. Edinburgh University Press.

Gouldner, A. W. (1959) Organizational analysis. In R.K. Merton, L. Broom & L.S. Cottrell Jr. *Sociology today: Problems and prospects*. Basic Books, Inc. New York.

Greenberger, D. B., Miceli, M. P., & Cohen, D. J. (1987). Oppositionists and group norms: The reciprocal influence of whistle-blowers and co-workers. *Journal of Applied Business Ethics, 6, 527*-542.

Gunasekaran, A., Khalil, O. & Rahman, S. M. (2003). *Knowledge and information technology management: Human and social perspectives*. Massachusetts: Idea Group.

Gundlach, M. J., Douglas, S. C., & Martinko, M. J. (2003) The decision to blow the whistle: A social information processing framework. *Academy of Management Review, 28*, 107-123.

Hall, R.H. (1977) *Organizations: Structure and process*. Englewood Cliffs, N.J.: Prentice Hall.

Hagen, J. M. & Choe, S. (1998). Trust in Japanese interfirm relations: Institutional sanctions matter. *Academy of Management Review, 23*, 589-600.

Haralambos, M. & Heald, R. (1985). *Sociology: Themes and perspectives*. Slough, UK: University Tutorial Press.

Hargie, O. D. W., Dickson, D. A., & Rainey, S. (2002). Religious difference, inter-group trust, attraction, and disclosure amongst young people in Northern Ireland. *International Journal of Adolescence and Youth, 10*, 213-235.

Haslam, S. A. (2004). *Psychology in organizations. The social identity approach.* London: Sage.

Haslam, S. A., Eggins, R. A., Reynolds, K. J. (2003). The ASPIRe model: Actualizing Social and Personal Identity Resources to enhance organizational outcomes. *Journal of Occupational and Organizational Psychology, 76*, 83-113.

Haslam, S. A. & McGarty, C. (2003). Experimental design and causality in social psychological research. In C. Sanson, C. C. Morf, & A. T. Panter (Eds.) *Handbook of methods in social psychology* (pp. 235-264). Thousand Oaks, CA: Sage.

Haslam, S. A., van Knippenberg, D., Platow, M. J., & Ellemers, N. (2003). *Social identity at work: Developing theory for organizational practice.* New York: Psychology Press.

Hendrick, S. (1987). Counseling and self-disclosure. In V. Derlega & J. Berg (Eds.) *Self-disclosure: Theory, research, and therapy* (pp. 303-327). New York: Plenum Press.

Hewstone, M. & Brown, R. J. (1986). Contact is not enough. An intergroup perspective of the contact hypothesis. In M. R. C. Hewstone & R. J. Brown (Eds.) *Contact and conflict in intergroup encounters* (pp. 1-44). Oxford: Blackwell.

Hill, C., Gelso, C. J., & Mohr, J. J. (2000) Client concealment and self-presentation in therapy: Comment on Kelly (2000). *Psychological Bulletin, 126*, 495-500.

Hill, C. T. & Stull, D. E. (1982). Disclosure reciprocity: Conceptual and measurement issues. *Social Psychology Quarterly, 45*, 238-244.

Hinge, A. (1996). The synergy of 'Jointery'. *Journal of the Australian Naval Institute, February/April*, 34-46.

Hogg, M. A. & Terry, D. J. (2000). Social identity and self-categorization processes in organizational contexts. *Academy of Management Review, 25*, 121-140.

Hook, M. K. & Cleveland, J. L. (1999). To tell or not to tell: Breaching confidentiality with clients with HIV and AIDS. *Ethics & Behavior, 9*, 365-381.

Hornsey, M. J. & Hogg, M. A. (1999). Subgroup differentiation as a response to an overly-inclusive group: A test of optimal distinctiveness theory. *European Journal of Social Psychology, 29*, 543-550.

Hornsey, M. J. & Hogg, M. A. (2000a). Subgroup relations: A comparison of multiple intergroup differentiation and common ingroup identity models of prejudice reduction. *Personality and Social Psychology Bulletin, 26*, 242-256.

Hornsey, M. J. & Hogg, M. A. (2000b). Assimilation and diversity: An integrative model of subgroup relations. *Personality and Social Psychology Review, 4*, 143-156.

Hoskinsson, R. E., Hitt, M. A., & Hill, C. W. L. (1991). Managerial risk taking in diversified firms: An evolutionary perspective. *Organization Science, 2*, 296-314.

Jacques, L. H. & Folen, R. A. (1998). Confidentiality and the military. Avoiding ethical misconduct in psychology specialty areas. In R. M. J. Anderson, T. L. Needels & H. V. Hall (Eds.) *Avoiding Ethical Misconduct In Psychology Specialty Areas* (pp. 247-257). Springfield: Charles C Thomas.

Janis, I. L. & Mann, L. (1977) *Decision making*. New York: Free Press.

Jetten, J., Spears, R., & Manstead, A. S. R. (1999). Group distinctiveness and intergroup discrimination. In N. Ellemers, R. Spears, & B. Doosje (Eds.) *Social identity: Context, commitment, content* (pp. 68-88). Oxford: Blackwell.

Jones, G. R. & George, J. M. (1998). The experience and evolution of trust: Implications for cooperation and teamwork. *Academy of Management Review, 23*, 531-546.

Jones, W. & Burdette, M. P. (1994). Betrayal in relationships. In A. Weber & J. Harvey (Eds.) *Perspectives on close relationships* (pp. 243-262). Boston: Allyn and Bacon.

Jos, P. H., Tompkins, M. E., & Hays, S. W. (1989). In praise of difficult people: A portrait of the committed whistle-blower. *Public Administration Review, 49*, 552-561.

Jourard, S. M. (1971). *Self-disclosure: An experimental analysis of the transparent self*. New York: Wiley-Interscience.

Kahneman, D. & Tversky, A. (1979). Prospect theory: An analysis of decision-making under risk. *Econometrica, 47*, 263-291.

Kahneman, D. & Tversky, A. (1982). The psychology of preferences. *Scientific American, 246*, 160-173.

Kaiser, F. M. (1980). Secrecy, intelligence, and community: The U.S. Intelligence Community. In S. K. Tefft. (Ed.) *Secrecy: A cross-cultural perspective* (pp. 273-297). Winston-Salem: Wake Forest University.

Katz, D. & Kahn, R. L. (1966). *The social psychology of organizations*. New York: Wiley.

Kelly, A. E. (2001). Revealing personal secrets. *Current Directions in Psychological Science, 8*, 105-108.

Kelly, A. E. (2002). *The psychology of secrets*. New York: Kluwer.

Kelly, A. E. & Carter, J. E. (2001). Dealing with secrets. In C. R. Snyder (Ed.) *Coping with stress: Effective people and processes*. Oxford: Oxford University Press.

Kelvin, P. (1973). A social-psychological examination of privacy. *British Journal of Social and Clinical Psychology*, 12: 248-261.

Kenworthy, J. B. (in press). Attitude threat, social identity, and consensus estimation [Manuscript submitted for publication].

Kessler, T. & Mummendey, A. (2001). Is there any scapegoat around? Determinants of intergroup conflicts at different categorization levels. *Journal of Personality and Social Psychology, 81*, 1090-1102.

Knowles, A. D. & McMahon, M. (1995). Expectations and preferences regarding confidentiality in the psychologist-client relationship. *Australian Psychologist, 30*, 175-178.

Komorita, S. S. & Parks, C. D. (1996). *Social dilemmas*. Boulder: Westview Press.

Kramer, R. M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual Review of Psychology, 50*, 569-598.

Kramer, R. M. (2001). Identity and trust in organizations: One anatomy of a productive but problematic relationship. In M. A. Hogg & D. J. Terry (Eds.) *Social identity processes in organizational contexts* (pp. 167-179). Sussex: Psychology Press.

Kramer, R. M., Brewer, M. & Hanna, B. (1996). Collective trust and collective action: The decision to trust as a social decision. In R. M. Kramer & T. R. Tyler (Eds.) *Trust in organizations: Frontiers of theory and research* (pp. 357-389). Thousand Oaks: Sage.

Kramer, R. M. & Tyler, T. R. (1996). *Trust in organizations: Frontiers of theory and research*. Thousand Oaks: Sage.

Lane, C. & Bachmann, R. (1996). The social constitution of trust: Supplier relations in Britain and Germany. *Organization Studies, 17*, 365-395.

Laufer, R. S. & Wolfe, M. (1977). Privacy as a concept and a social science: A multidimensional development theory. *Journal of Social Issues, 33*, 22-35.

Lawson, B. & Samson, D. (2002). Developments in managing innovation, knowledge, and e-business. In A. Gunasekaran, O. Khalil, & S. M. Rahman (Eds.) *Knowledge and information technology management: Human and social perspectives* (pp. 1-13). Massachusetts: Idea Group.

Lea, M., Spears, R., & Rogers, P. (2003). Social process in electronic teamwork: The central issue of identity. In S. A. Haslam, D. van Knippenberg, M. J. Platow, and N. Ellemers (Eds.) *Social identity at work: Developing theory for organizational practice* (pp. 99-115). New York: Psychology Press.

Levchenko, S. (1988). *On the wrong side: My life in the KGB.* Washington: Pergamon-Brassey's International Defense Publishers.

Levy, A., Laska, F., Abelhauser, A., Delfraissey, J-F., Goujard, C., Boue F., et al. (1999). Disclosure of HIV seropositivity. *Journal of Clinical Psychology, 55,* 1041-1049.

Lewicki R. J. & Bunker, B. B. (1995). Trust in relationships: A model of development and decline. In B. B. Bunker and J. Z. Rubin (Eds.) *Conflict, cooperation and justice: Essays inspired by the work of Morton Deutsch* (pp: 133-173). San Francisco: Jossey-Bass.

Lewis J. D. & Weigert, A. (1985). Trust as a social reality. *Social Forces, 63,* 967-985.

Lindethal, J. J., Amaranto, E. A., Jordan, T. J., & Wepman, B. J. (1984). Decisions about confidentiality in medical student mental health settings. *Journal of Counseling Psychology, 31,* 572-575.

Lindethal, J. J., Jordan, T. J., Lentz, J. D., & Thomas, C. S. (1988). Social worker's management of confidentiality. *Social Work, 33,* 157-158.

Lindethal, J. J. & Thomas, C. S. (1980). A comparative study of the handling of confidentiality. *The Journal of Nervous and Mental Disease, 168,* 361-369.

Loomes, G., Starmer, C., & Sugden, R. (1992). Are preferences monotonic? Testing some implications of regret theory. *Economica, 59,* 17-33.

Loomes, G. & Sugden, R. (1982). Regret theory: An alternative theory of rational choice under uncertainty. *Economic Journal, 92,* 805-892.

Lopes, L. L. (1987). Between hope and fear: The psychology of risk. In L. Berkowitz (Ed.) *Advances in experimental and social psychology* (pp. 255-295). San Diego: Academic Press.

Lowry, R. P. (1972). Toward a sociology of secrecy and security systems. *Social Problems, 19*, 437-450.

Luce, R. D. & Raiffa, H. (1957, 1989). *Games and decisions*. New York: Wiley.

MacCrimmon, K. R. & Wehrung, D. A. (1986). *Taking risks: The management of uncertainty*. New York: Free Press.

MacDonald, A. P., Kessel, V. S., & Fuller, J. B. (1972). Self-disclosure and two kinds of trust. *Psychological Reports, 30*, 143-148.

MacKenzie, N. (1967). *Secret societies*. New York: Holt, Rinehart and Winston.

Madhok, A. (1995). Revisiting multinational forms' tolerance for joint ventures: A Trust-based approach. *Journal of International Business Studies, 26*, 117-137.

Mael, F. A. & Ashforth, B. E. (1992). Alumni and their alma mater: A partial test of the reformulated model of organizational identification. *Journal of Organizational Behavior, 13*, 103-123.

March, J. G. & Shapira, Z. (1987). Managerial perspectives on risk and risk-taking. *Management Science, 33*, 1404-1418.

March, J. G. & Simon, H. A. (1958). *Organizations*. New York: J. Wiley.

Margulis, S.T. (1977). Conceptions of privacy: Current status and next steps. *The Journal of Social Issues*, 33(3): 5-22.

Marr, D. & Wilkinson, M. (2003). *Dark victory*. Crow's Nest: Allen & Unwin.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*, 709-734.

McAllister, A. & Kiesler, D. J. (1975). Interviewee disclosure as a function of interpersonal trust, task modeling, and interviewer self-disclosure. *Journal of Consulting and Clinical Psychology, 43*, 428.

McAllister, D. J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal, 38*, 24-59.

McCauley, D. P. & Kuhnert, K. W. (1992). A theoretical review and empirical investigation of employee trust. *Public Administration Quarterly, 16*, 265-285.

McGarty, C. (2001). Social Identity Theory does not maintain that identification produces bias and Self-categorization Theory does not maintain that salience is identification: Two comments on Mummendey, Klink, and Brown. *British Journal of Social Psychology, 40*, 173-176.

McGarty, C. & Bliuc, A-M. (2004). Refining the meaning of the "Collective" in collective guilt: Harm, guilt, and apology in Australia. In N. R. Branscombe & B. Doosje (Eds.) *Collective guilt: International perspectives* (pp. 112-129). New York: Cambridge University Press.

McGarty, C., Yzerbyt, V. Y., & Spears, R. (2002). *Stereotypes as explanations: The formation of meaningful beliefs about social groups*. Cambridge: Cambridge University Press.

Mellers, B., Schwartz, A., & Ritov, I. (1999). Emotion-based choice. *Journal of Experimental Psychology: General, 128*, 332-345.

Merten, D.E. (1999). Enculturation into secrecy among junior high school girls. *Journal of Contemporary Ethnography, 28*, 107-137.

Messick, D.M. (1999). Dirty secrets: Strategic uses of ignorance and uncertainty. In L. L. Thompson, J. M. Levine & D. M. Messick (Eds.) *Shared cognition in organizations: The management of knowledge* (pp. 71-87). New York: Lawrence Erlbaum.

Messick, D. M. & Mackie, D. M. (1989) Intergroup relations. *Annual Review of Psychology, 40*, 45-81.

Meyerson, D., Weick, K. & Kramer, R. (1996). Swift trust and temporary groups. In R. M. Kramer & T. R. Tyler (Eds.) *Trust in organizations: Frontiers of theory and research* (pp. 166-195). Thousand Oaks: Sage.

Miceli, M. P., Dozier, J. B., & Near, J. P. (1991). Blowing the whistle on data-fudging: A controlled field-experiment. *Journal of Applied Social Psychology, 21*, 271-295.

Miceli, M. P. & Near, J. P. (1988). Individual and situational correlates of whistle-blowing. *Personnel Psychology, 41*, 267-281.

Mikulincer, M. & Nachshon, O. (1991). Attachment styles and patterns of self-disclosure. *Journal of Personality and Social Psychology, 61*, 321-331.

Milicki, P. P. & Ellemers, N. (1996). Being different or being better? National stereotypes and identifications of Polish and Dutch students. *European Journal of Social Psychology, 26*, 97-114.

Miller, R. J. & Boon, S. D. (2000). Trust and disclosure of sexual orientation in gay males' mother-son relationships. *Journal of Homosexuality, 38*, 41-63.

Mongin, P. (1997). Expected utility theory. In J. Davis, W. Hands, & U. Maki (Eds.) *Handbook of economic methodology* (pp. 342-350). London: Edward Elgar.

Montgomery, D. (1991). How the A-12 went down. *Air Force, 74*, 1-7.

Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research, 27*, 323-339.

Morris, J. H. & Moberg, D. J. (1994). Work organizations as contexts for trust and betrayal. In T. R. Sarbin, R. M. Carney, & E. Eoyang (Eds.) *Citizen espionage: Studies in trust and betrayal* (pp. 163-187). Westport: Greenwood.

Moser, P. K. (1990). Rationality in action: General introduction. In P. K. Moser *Rationality in action: Contemporary approaches* (pp. 1-10). Cambridge: Cambridge University Press.

Moynihan, D. P. (1998). *Secrecy: The American experience.* New Haven: Yale University Press.

Mullen, B, Brown, R., & Smith, C. (1992). Ingroup bias as a function of salience, relevance, and status: An integration. *European Journal of Social Psychology, 22*, 103-122.

Near, J. P. & Miceli, M. P. (1985). Organizational dissidence: The case of whistle-blowing. *Journal of Business Ethics, 4*, 1-16.

Near, J. P. & Miceli, M. P. (1996). Whistle-blowing: Myth and reality. *Journal of Management, 22*, 507-526.

Nowell, D., & Spruill, J. (1993). If it's not absolutely confidential, will the information be disclosed? *Professional Psychology – Research & Practice, 24*, 367-369.

Oakes, P. J. (1987). The salience of social categories. In J. C. Turner, M. A. Hogg, P. J. Oakes, S. D. Reicher, & M. S. Wetherell (Eds.) *Rediscovering the social group: A self-categorization theory* (pp. 117-141). Oxford: Blackwell.

Oakes, P. J., Haslam, S. A., & Turner, J. C. (1994). *Stereotyping and social reality.* Oxford: Blackwell.

Onorato, R. S. & Turner, J. C. (2001). The "I", the "me", and the "us": The psychological group and self-concept maintenance and change. In C. Sedikides & M. Brewer (Eds.) *Individual self, relational self, collective self* (pp. 147-170). Philadelphia: Psychology Press.

Onorato, R. S. & Turner, J. C. (2002). Challenging the primacy of the personal self: The case for depersonalized self-conception. In Y. Kashima, M. Foddy, & M. Platow (Eds.) *Self and identity: Personal, social, and symbolic* (pp. 145-178). Mahwah: Lawrence Erlbaum Associates.

Orbell, J., Dawes, R., & Schwartz-Shea, P. (1994). Trust, social categories, and individuals: The case of gender. *Motivation and Emotion, 18*, 109-128.

Owens, W. A. (1993-94). Living Jointness. *Joint Force Quarterly, Winter*, 7-14.

Petronio, S. (1999). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory, 1*, 311-335.

Petronio, S. & Bantz, C. (1991). Controlling the ramifications of disclosure: "Don't tell anybody but..." *Journal of Language and Social Psychology, 10*, 263-269.

Petronio, S., Reeder, H. M., Hecht, M. L., & Mon't Ros-Mendoza, T. (1996) Disclosure of sexual abuse by children and adolescents. *Journal of Applied Communication Research, 24*, 181-199.

Pettigrew, A. M. (1972). Information control as a power resource. *Sociology, 6*, 187-204.

Pistole, M. C. (1993). Attachment relationships: Self-disclosure and trust. *Journal of Mental Health Counseling, 15*, 94-106.

Ponse, B. (1976). Secrecy in the lesbian world. *Urban Life, 5*, 313-338.

Postmes, T. (2001). A social identity approach to communication in organizations. In S. A. Haslam, D. van Knippenberg, M. J. Platow, & N. Ellemers (Eds.) *Social identity at work: Developing theory for organizational practice* (pp. 81-97). New York: Psychology Press.

Poston, W. C., Craine, M., & Atkinson, D. R. (1991). Counselor dissimilarity confrontation, client cultural mistrust, and willingness to self-disclose. *Journal of Multicultural Counseling and Development, 19*, 65-73.

Redlinger, L. J. & Johnson, S. (1980) Secrecy, informational uncertainty, and social control. *Urban Life, 8*, 387-397.

Reynolds, K. J., Turner, J. C., & Haslam, S. A. (2003). Social identity and self-categorization theories' contribution to understanding identification, salience, and diversity in teams and organizations. In J. Polzer (Ed.) *Identity issues in groups: Research on managing groups and teams* (Vol 5, pp. 279-304). Oxford: JAI Elsevier Science.

Roberts, K. H. & O'Reilly, C. (1974). Failures in upward communication in organizations: Three possible culprits. *Academy of Management Review, 17*, 205-215.

Roccas, S. & Schwartz, S. H. (1993). Effects of intergroup similarity on intergroup relations. *European Journal of Social Psychology, 23*, 581-95.

Rotenberg, K. J. (1986). Same-sex patterns and sex differences in the trust-value basis of children's friendship. *Sex Roles, 15*, 613-626.

Rothschild, J. & Miethe, T. D. (1999). Whistle-blower disclosures and management retaliation. *Work and Occupations*, 26, 107-128.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality*, 35, 651-665.

Rousseau, D., Sitkin, S., Burt, R., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*, 393-404.

Rumsfeld, D. (2002). *The Impact Of Leaking Classified Information* (U.S. Department of Defense Minute: U11159/02). Department of Defense.

Sarbin, T. R., Carney, R. M., & Eoyang, E. (1994). *Citizen espionage: Studies in trust and betrayal.* Westport CT: Praeger.

Sapolsky, H. M. (1997). Interservice competition: The solution, not the problem. *Joint Force Quarterly*, *Spring,* 50-53.

Sauka, M. & Lie, G. T. (2000) Confidentiality and the disclosure of HIV infection: HIV-positive persons' experience with HIV testing and coping with HIV infection in Latvia. *AIDS Care*, *12*, 737-743.

Savage, L. J. (1954). *The foundations of statistics.* New York: Dover.

Sawyer, J. E. (1990). Effects of risk and ambiguity on judgments of contingency relations and behavioral resource allocation decisions. *Organizational Behavior and Human Decision Processes*, *45*, 85-110.

Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology*, *73*, 741-752.

Scott, W. R. (1992). *Organizations: Rational, natural, and open systems.* Englewood Cliffs: Prentice Hall.

Seta, C. E., Seta, J. J., & Culver, J. (2000). Recategorization as a method for promoting intergroup cooperation. Group status matters. *Social Cognition*, *18*, 354-376.

Shapira, Z. (1995). *Risk taking: A managerial perspective.* New York: Russell Sage Foundation.

Shils, E. (1956). *The torment of secrecy.* Glencoe. Free Press.

Shlien, J. M. (1984). Secrets and the psychology of secrecy. In R. F. Levant & J. M. Shlien (Eds.) *Client-centred therapy and the person-centred approach: New directions in theory, research, and practice* (pp. 390-399). New York: Praeger.

Simmel, G. (1906). The sociology of the secret and of secret societies. *The American Journal of Sociology, 11*, 441-498.

Simmel, G. (1950). *The sociology of Georg Simmel.* New York: MacMillan.

Simone, S. J. & Fulero, S. M. (2001). Psychologists' perceptions of their duty to protect uninformed sex partners of HIV-positive clients. *Behavioral Sciences and the Law, 19*, 423-436.

Simonson, I. (1992). The influence of anticipating regret and responsibility on purchase decisions. *Journal of Consumer Research, 19*, 105-118.

Smith, H. A. & McKeen, J. D. (2003). Instilling a knowledge-sharing culture. (*Report* WP 03-11). Queen's Centre for Knowledge-Based Enterprises. Queen's University at Kingston, Ontario.

Smithson, M. J. (1994). Uncertainty. In V. S. Ramachandran (Ed.) *Encyclopedia of Human Behavior* (pp. 437-446). New York: Academic Press.

Smithson, M. J. & Foddy, M. (1999). Theories and strategies for the study of social dilemmas. In M. Foddy, M. Smithson, S. Schneider, & M. Hogg (Eds.) *Resolving Social Dilemmas: Dynamic, Structural, and Intergroup Aspects* (pp. 1-14). Philadelphia: Psychology Press.

Spears, R., Doosje, B. & Ellemers, N. (1997). Self-stereotyping in the face of threats to group status and distinctiveness: The role of group identification. *Personality and Social Psychology Bulletin, 23*, 538-553.

Steel, J. L. (1991). Interpersonal correlates of trust and self-disclosure. *Psychological Reports, 68*, 1319-1320.

Steele, F. (1975). *The open organization: The impact of secrecy and disclosure on people and organizations*. Reading: Addison-Wesley.

Stevenson, R. B. (1980). *Corporations and information: Secrecy, access, and disclosure*. New York: Free Press.

Street, M. D. (1995). Cognitive moral development and organizational commitment: Two potential predictors of whistle-blowing. *Journal of Applied Business Research, 11*, 104-115.

Sugden, R. (1985). Regret, recrimination, and rationality. *Theory and Decision, 19*, 77-99.

Suzuki, S. (1998). In-group and out-group communication patterns in international organizations: Implications for social identity theory. *Communication Research, 25*, 154-182.

Tajfel, H. (1970). Experiments in intergroup discrimination. *Scientific American, 223*, 96-102.

Tajfel, H. (1972). La categorisation sociale (English trans.). In S. Moscovici (Ed.) *Introduction a la psychologie sociale*. Paris: Larouse.

Tajfel, H. (1978). Social categorization, social identity and social comparison. In H. Tajfel (Ed.) *Differentiation Between Social Groups* (pp. 61-77). London: Academic Press.

Tajfel, H., Flament, C., Billig, M. G., & Bundy, R. F. (1971). Social categorization and intergroup behaviour. *European Journal of Social Psychology, 1*, 149-177.

Tajfel, H. & Turner, J. C. (1979). An integrative theory of social conflict. In W.G. Austin & S. Worchel (Eds.) *The Social Psychology of Intergroup Relations* (pp. 33-47). Monterey: Brooks-Cole.

Tajfel, H. & Turner, J.C. (1986). The social identity theory of intergroup behavior. In S. Worchel & W.G. Austin (Eds.) *Psychology of Intergroup Relations.* Chicago: Nelson-Hall.

Taylor, L. & Adelman, H.S. (1989). Reframing the confidentiality dilemma to work in children's best interests. *Professional Psychology: Research And Practice, 20,* 79-83.

Taylor, S. A. & Snow, D. (1997). Cold war spies: Why they spied and how they got caught. *Intelligence and National Security, 12*, 101-125.

Tefft, S. K. (1980). *Secrecy: A cross-cultural perspective.* New York: Human Sciences Press.

Thompson, J. D. (1967). *Organizations in action.* New York: McGraw Hill.

Trainor, B. E. (1993-4). Jointness, service culture, and the Gulf War. *Joint Force Quarterly, Winter*, 74.

Tsoukas, H. (1998). Forms of knowledge and forms of life in organized contexts. In R. C. H. Chia (Ed.) *In the realm of organizations: Essays for Robert Cooper.* London. Routledge.

Tsoukas, H. (2001) Re-viewing organization. *Human Relations*, 54(1): 7-12.

Turner, J. C. (1975). Social comparison and social identity: Some prospects for intergroup behaviour. *European Journal of Social Psychology, 5*, 5-34.

Turner, J. C. (1978a). Social comparison, similarity, and ingroup favouritism. In H. Tajfel (Ed.) *Differentiation Between Social Groups* (pp. 235-250). London: Academic Press.

Turner, J. C. (1978b). Social categorization and social discrimination in the minimal group paradigm. In H. Tajfel (Ed.) *Differentiation Between Social Groups* (pp. 101-140). London: Academic Pres.

Turner, J. C. (1981). The experimental social psychology of intergroup behaviour. In J. C. Turner & H. Giles (Eds.) *Intergroup Behaviour* (pp. 66-101). Oxford: Basil Blackwell.

Turner, J. C. (1981b). Some considerations in generalizing experimental social psychology. In G. M. Stephenson & J. H. Davis (Eds.) *Progress in applied social psychology* (Vol. 1, pp. 3-34).

Turner, J. C. (1982). Towards a cognitive redefinition of the social group. In H. Tajfel (Ed.) *Social identity and intergroup relations* (pp. 15-40). Cambridge: Cambridge University Press.

Turner, J. C. (1985). Social categorization and the self-concept. A social cognitive theory of group behaviour. In E. J. Lawler (Ed.) *Advances in Group Processes* (Vol. 2, pp. 77-122). Greenwich: JAI Press.

Turner, J. C. (1991). *Social influence.* Milton-Keynes: Open University Press.

Turner, J. C. (1999). Some current issues in research on social identity and self-categorization theories. In N. Ellemers, R. Spears, & B. Doosje (Eds.) *Social identity: Context, commitment, content* (pp. 6-34). Oxford: Blackwell.

Turner, J. C. & Bourhis, R. Y. (1996). Social identity, interdependence and the social group: A reply to Rabbie et al. In W. Peter Robinson (Ed.) *Social Groups and Identities: Developing the Legacy of Henri Tajfel* (pp. 25-63). Oxford: Butterworth Heinemann.

Turner, J. C. & Brown, R. Y. (1978). Social status, cognitive alternatives, and intergroup relations. In H. Tajfel (Ed.) *Differentiation between social groups* (pp. 201-234). London: Academic Press.

Turner, J. C. & Haslam, S. A. (2001). Social identity, organizations, and leadership. In M. E. Turner (Ed.) *Groups at work: Theory and research* (pp. 25-65). Mahwah: Erlbaum.

Turner, J. C., Hogg, M. A., Oakes, P. J., Reicher, S. D., & Wetherell, M. S. (1987). *Rediscovering the social group: A self-categorization theory*. Oxford: Blackwell.

Turner, J. C., Oakes, P. J., Haslam, S. A., & McGarty, C. A. (1994). Self and collective: Cognition and social context. *Personality and Social Psychology Bulletin, 20*, 454-463.

Turner, J. C. & Onorato, R. S. (1999). Social identity, personality, and the self-concept: A self-categorization perspective. In T. R. Tyler, R. M. Kramer, and O. P. John (Eds.) *The psychology of the social self* (pp. 11-46). Mahwah: Lawrence Erlbaum Associates.

Turner, J. C. & Reynolds, K. J. (2001). The social identity perspective in intergroup relations: Theories, themes and controversies. In R. Brown & S. Gaertner (Eds.) *Blackwell Handbook of Social Psychology: Intergroup Processes* (pp. 133-152). Oxford: Blackwell.

Tyler, T. R. (1999). Why people cooperate with organizations: An identity-based perspective. In B. M. Staw & R. Sutton (Eds.) *Research in organizational behaviour* (Vol. 21, pp. 201-246). Greenwich: JAI Press.

Tyler, T. R. (2001). Cooperation in organizations: A social identity perspective. In M. A. Hogg & D. J. Terry (Eds.) *Social identity processes in organizational contexts* (pp. 149-165). Philadelphia: Psychology Press.

Tyler, T. R. & Blader, S. L. (2000). *Cooperation in groups: Procedural justice, social identity and behavioral engagement*. Philadelphia. Psychology Press.

Tyler, T. R. & Blader, S. L. (2001). Identity and cooperative behavior in groups. *Group processes & Intergroup Relations*, *4*, 207-226.

United States Department of Homeland Security. (2004). *Securing our homeland: U.S. Department of Homeland Security Strategic Plan*. U.S. Department of Homeland Security.

United States Department of Justice. (2003). *The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information.* (Audit Report 04-10). U.S. Department of Justice.

United States House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. (2002). *Joint inquiry into Intelligence Community activities before and after the terrorist attacks of September 11, 2001.* (S Rept. No. 107-351). Washington DC: U.S. Government Printing Office.

Vandecreek, L. & Knapp, S. (2001). *Tarasoff and beyond: Legal and clinical considerations in the treatment of life-endangering patients*. Sarasota: Professional Resource Press.

Vandivier, K. (1972) *"Why Should My Conscience Bother Me?": In the name of profit*. NY: Doubleday & Co.

Vangelisti, A. L. & Caughlin, J. P. (1997). Revealing family secrets: The influence of topic, function and relationships. *Journal of Social and Personal Relationships, 14*, 679-705.

van Knippenberg, D. & Sleebos, E. P. (1999). Identification, commitment, and individualism-collectivism: Their interrelations and relationship with organizational citizenship behavior. [*Unpublished manuscript. University of Amsterdam*].

van Leeuwin, E. & van Knippenberg, D. (2003). Organization identification following a merger: The importance of agreeing to differ. In S. A. Haslam, D. van Knippenberg, M. J. Platow, and N. Ellemers (Eds.) *Social identity at work: Developing theory for organizational practice* (pp. 205-221). New York: Psychology Press.

van Leeuwin, E., van Knippenberg, D., & Ellemers, N. (2001). The merits of a merger mismatch. Shifts in identification from pre- to post-merger group membership. [*Unpublished manuscript, Leiden University*].

Veenstra, K. E. (2003). The psychology of precarious employment: Security, status, and social identification. [*Unpublished manuscript. Australian National University*].

Vlek, C. & Stallen, P-J. (1980). Rational and personal aspects of risk. *Acta Psychologica, 45*, 273-300.

Vondracek, F. W. & Marshall, M. J. (1971). Self-disclosure and interpersonal trust: An exploratory study. *Psychological Reports, 28*, 235-240.

von Neumann, J. & Morgenstern, O. (1944). *Theory of games and economic behavior.* Princeton: Princeton University Press.

Vrij, A., Nunkoosing, K., Paterson, B., Oosterwegel, A., & Soukara, S. (2002). Characteristics of secrets and the frequency, reasons and effects of secrets keeping and disclosure. *Journal of Community and Applied Social Psychology*, *12*, 56-70.

Vrij, A., Paterson, B., Nunkoosing, K., Soukara, S., & Oosterwegel, A. (2003). Perceived advantages and disadvantages of secrets disclosure. *Personality & Individual Differences*, *35*, 593-602.

Wagner, D. G. & Berger, J. (1985). Do sociological theories grow? *American Journal of Sociology*, *90*, 697-728.

Wagner, R. K. & Sternberg, R. J. (1987). Tacit knowledge in managerial success. *Journal of Business & Psychology*, *1*, 301-312.

Warne, L., Agostino, K., Ali, I., Pascoe, C., & Bopping, D. (2003). The knowledge edge: Knowledge management and social learning in military settings. In A. Gunasekaran, O. Khalil, & S. M. Rahman (Eds.) *Knowledge and information technology management: Human and social perspectives* (pp. 324-353). Massachusetts: Idea Group.

Warne, L., Ali, I., Bopping, D., Hart, D., & Pascoe, C. (2003). *The network centric warrior* (DSTO Report 10/2003). Commonwealth of Australia.

Watkins, S.A. (1989). Confidentiality: An ethical and legal conundrum for family therapists. *The American Journal of Family Therapy*, *17*, 291-302.

Warren, C. & Laslett, B. (1977). Privacy and secrecy: A conceptual comparison. *Journal of Social Issues*, *33*, 43-51.

Weber, M. (1946). *On Max Weber: Essays in sociology*. New York: Oxford University Press.

Wetzel, C. G. & Wright-Buckley, C. (1988). Reciprocity of self-disclosure: Breakdowns of trust in cross-racial dyads. *Basic and Applied Social Psychology, 9*, 277-288.

Wheeless, L. R. (1978). A follow-up study of the relationships among trust, disclosure, and interpersonal solidarity. *Human Communication Research, 4*, 143-157.

Wheeless, L. R; Erickson, K. V., & Behrens, J. S. (1986). Cultural differences in disclosiveness as a function of locus of control. *Communication Monographs, 53*, 36-46.

Wheeless, L. R. & Grotz, J. (1977). The measurement of trust and its relationship to self-disclosure. *Human Communication Research, 3*, 250-257.

Wigboldus, D., Spears, R., Semin, G. (1999). Categorization, content and the context of communicative behaviour. In N. Ellemers, R. Spears, & B. Doosje (Eds.) *Social identity: Context, commitment, content* (pp. 147-163). Oxford: Blackwell.

Wilkerson, L. B. (1997). What exactly is Jointness? *Joint Force Quarterly, Summer*, 66-68.

Williams, M. (2001). In whom we trust: Group membership as an affective context for trust development. *Academy of Management Review, 26*, 377-396.

Wilsnack, R.W. (1980). Information control: A conceptual framework for sociological analysis. *Urban Life, 8*, 467-499.

Wilson, C. (2004). Network centric warfare: Background and oversight issues for Congress. (*CRS Report for Congress RL32411*). Congressional Research Service. The Library of Congress.

Wit, A. P. & Wilke, H. A. M. (1992). The effect of social categorization on cooperation in three types of social dilemmas. *Journal of Economic Psychology, 13*, 135-151.

Yamagishi, T., Foddy, M., Makimura, Y., Matuda, M., & Platow, M. (2003). Contextualized and decontextualized use of social categories: Comparisons of Australians and Japanese on group-based trust and cooperation. Unpublished manuscript.

Yates, J. F. & Stone, E. R. (1992). The risk construct. In J. F. Yates (Ed.) *Risk-taking Behavior* (pp. 1-25). New York: Wiley.

Yovetich, N. A. & Drigotas, S. M. (1999). Secret transmission: A relative intimacy hypothesis. *Personality and Social Psychology Bulletin, 25*, 1135-1146.

Zand, D. E. (1972). Trust and managerial problem solving. *Administrative Science Quarterly, 17*, 229-239.

Zeelenberg, M. (1999). Anticipated regret, expected feedback and behavioral decision-making. *Journal of Behavioral Decision Making, 12*, 93-106.

APPENDIX A

DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION
DSTO

RESEARCH ON TRUST AND DISCLOSURE WITHIN THE STRATEGIC DEFENCE ENTERPRISE

Introduction

The knowledge environment of the ADF, especially as it relates to C3I decision-making, depends primarily upon the disclosure and non-disclosure of information within and between its elements. The aim of this study is to investigate how strategic-level ADF personnel make decisions about disclosing information within the Defence enterprise. Gaining an awareness of such decision-making will begin to provide a deeper understanding of the Defence knowledge environment.

This study is part of a broader research program within Joint Systems Branch, DSTO, and is expected to complement work being conducted under the Enterprise Social Learning Architectures Task (JNT 98/004) and the ADF Cultural Survey. It also forms part of a PhD being conducted at the ANU.

Please be assured that participation in this research is entirely on a **voluntary** basis and that all information you provide is **anonymous** and **confidential**. If you have any questions relating to this study or would like more information about the broader research program, please don't hesitate to contact me.

Derek Bopping
Joint Systems Branch,
DSTO
02-6265-8826
derek.bopping@dsto.defence.gov.au

INSTRUCTIONS

1. Please read the hypothetical scenarios and the associated 'dilemmas' as they are presented in turn.

2. Then respond to the questions following each dilemma, by circling a number, ticking a box, or marking a line, where indicated.

3. Upon completion of the dilemmas, please fill-in the 'General Attitudes' and 'Participant Details' sections.

4. You may provide any comments on the final page.

This questionnaire should take around **15 minutes** to complete.

A NOTE ABOUT THE DILEMMAS

5. Some of the hypothetical dilemmas presented here entail decisions that may be more difficult to make compared to others.

   In those dilemmas it is appreciated that you would usually want to obtain more information before making decisions.

   Please assume though that in all these dilemmas the information you are presented is all that is available.

SCENARIO A

Scenario A below provides the backdrop to Dilemmas **1 – 4**.

In the course of your normal working week you meet regularly with an ADF friend to informally discuss strategic-level Defence projects.

On this particular occasion, your friend shares with you some information outlining upcoming changes to the funding of certain projects. These changes would immediately interrupt a number of major projects with important force structure and capability implications.

Your friend informs you that this information is reliable and trusts you not to provide the information to others.

DILEMMA 1

Imagine yourself in **Scenario A** and you now face a dilemma where:-

Providing the information to others will permanently damage the valued relationship you have established with your ADF friend who has trusted you not to disclose the information, yet…

Not providing the information to others will cause an ADF colleague from another work area within your Headquarters to make a bad decision that will unfairly limit their career advancement prospects.

(a) In this dilemma, how important do you think it is to maintain the trust of your ADF friend who provided you with the information? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(b) In this dilemma, how important do you think it is to provide the information to others? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(c) What would you decide in this dilemma? *(please tick only one box)*

☐ I **would not** provide the information to others

☐ I **would** provide the information to others

(d) What percentage of peers from your Headquarters would you expect to decide *as you did* in this dilemma? *(please mark the line with an 'X' at any point)*

(e) How confident are you that your decision in this dilemma is the most appropriate decision? *(please circle one number)*

Not at all confident 1 2 3 4 5 6 7 Very confident

DILEMMA 2

Again, imagine yourself in **Scenario A** and you now face a dilemma where:-

Providing the information to others will permanently damage the valued relationship you have established with your ADF friend who has trusted you not to disclose the information, yet...

Not providing the information to others will result in a significant and costly disruption to the implementation of a major project belonging to **your** Service.

(a) In this dilemma, how important do you think it is to maintain the trust of your ADF friend who provided you with the information? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(b) In this dilemma, how important do you think it is to provide the information to others? *(please circle one number)*

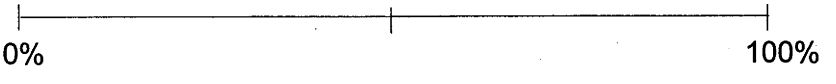
Not at all important 1 2 3 4 5 6 7 Very important

(c) What would you decide in this dilemma? *(please tick only one box)*

☐ I **would not** provide the information to others

☐ I **would** provide the information to others

(d) What percentage of peers from your Headquarters would you expect to decide *as you did* in this dilemma? *(please mark the line with an 'X' at any point)*



(e) How confident are you that your decision in this dilemma is the most appropriate decision? *(please circle one number)*

Not at all confident 1 2 3 4 5 6 7 Very confident

DILEMMA 3

Again, imagine yourself in **Scenario A** and you now face a dilemma where:-

Providing the information to others will permanently damage the valued relationship you have established with your ADF friend who has trusted you not to disclose the information, yet...

Not providing the information to others will result in a significant and costly disruption to the implementation of a major project belonging to **another** Service.

(a) In this dilemma, how important do you think it is to maintain the trust of your ADF friend who provided you with the information? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(b) In this dilemma, how important do you think it is to provide the information to others? *(please circle one number)*

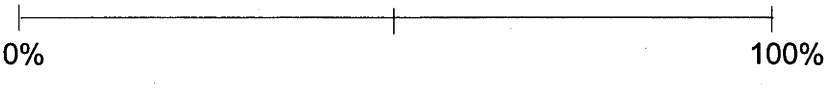
Not at all important 1 2 3 4 5 6 7 Very important

(c) What would you decide in this dilemma? *(please tick only one box)*

☐ I **would not** provide the information to others

☐ I **would** provide the information to others

(d) What percentage of peers from your Headquarters would you expect to decide *as you did* in this dilemma? *(please mark the line with an 'X' at any point)*



(e) How confident are you that your decision in this dilemma is the most appropriate decision? *(please circle one number)*

Not at all confident 1 2 3 4 5 6 7 Very confident

DILEMMA 4

Again, imagine yourself in **Scenario A** and you now face a dilemma where:-

Providing the information to others will permanently damage the valued relationship you have established with your ADF friend who has trusted you not to disclose the information, yet…

Not providing the information to others will lead to a situation in which certain strategic and operational areas of the ADF will be severely compromised in their ability to achieve key goals, and will likely lead to an increased risk of casualties to ADF personnel.

(a) In this dilemma, how important do you think it is to maintain the trust of your ADF friend who provided you with the information? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(b) In this dilemma, how important do you think it is to provide the information to others? *(please circle one number)*

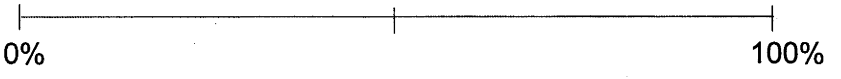
Not at all important 1 2 3 4 5 6 7 Very important

(c) What would you decide in this dilemma? *(please tick only one box)*

☐ I **would not** provide the information to others

☐ I **would** provide the information to others

(d) What percentage of peers from your Headquarters would you expect to decide *as you did* in this dilemma? *(please mark the line with an 'X' at any point)*



(e) How confident are you that your decision in this dilemma is the most appropriate decision? *(please circle one number)*

Not at all confident 1 2 3 4 5 6 7 Very confident

SCENARIO B

Scenario B below provides the backdrop to Dilemmas **5 - 8**

In the course of your normal work duties you are involved in the development and management of a range of strategic-level Defence projects.

On this particular occasion your work area provides you with some information outlining upcoming changes to the structure and staffing of certain projects. These changes would immediately interrupt a number of major projects with important force structure and capability implications.

Your work area informs you this information is reliable and you are directed not to provide the information to others outside your work area.

DILEMMA 5

Imagine yourself in **Scenario B** and you now face a dilemma where:-

Providing the information to others outside your work area will break the confidence it had established. This will result in you receiving an informal reprimand which will not be explicitly referred to on your annual report, but may affect your immediate career advancement prospects, yet...

Not providing the information to others outside your work area will cause an ADF colleague from another work area within your Headquarters to make a bad decision that will unfairly limit their career advancement prospects.

(a) In this dilemma, how important do you think it is to maintain the confidence established by your work area? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(b) In this dilemma, how important do you think it is to provide the information to others outside your work area? *(please circle one number)*

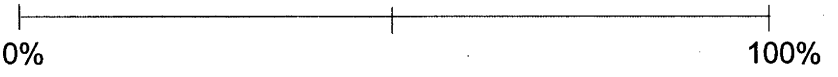
Not at all important 1 2 3 4 5 6 7 Very important

(c) What would you decide in this dilemma? *(please tick only one box)*

☐ I **would not** provide the information to others outside my work area

☐ I **would** provide the information to others outside my work area

(d) What percentage of peers from your Headquarters would you expect to decide *as you did* in this dilemma? *(please mark the line with an 'X' at any point)*



(e) How confident are you that your decision in this dilemma is the most appropriate decision? *(please circle one number)*

Not at all confident 1 2 3 4 5 6 7 Very confident

DILEMMA 6

Again, imagine yourself in **Scenario B** and you now face a dilemma where:-

Providing the information to others outside your work area will break the confidence it had established. This will result in you receiving an informal reprimand which will not be explicitly referred to on your annual report, but may affect your immediate career advancement prospects, yet...

Not providing the information to others outside your work area will result in a significant and costly disruption to the implementation of a major project belonging to **your** Service.

(a) In this dilemma, how important do you think it is to maintain the confidence established by your work area? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(b) In this dilemma, how important do you think it is to provide the information to others outside your work area? *(please circle one number)*

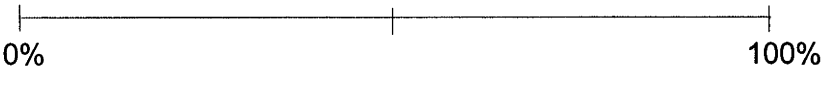
Not at all important 1 2 3 4 5 6 7 Very important

(c) What would you decide in this dilemma? *(please tick only one box)*

☐ I **would not** provide the information to others outside my work area

☐ I **would** provide the information to others outside my work area

(d) What percentage of peers from your Headquarters would you expect to decide *as you did* in this dilemma? *(please mark the line with an 'X' at any point)*



(e) How confident are you that your decision in this dilemma is the most appropriate decision? *(please circle one number)*

Not at all confident 1 2 3 4 5 6 7 Very confident

DILEMMA 7

Again, imagine yourself in **Scenario B** and you now face a dilemma where:-

Providing the information to others outside your work area will break the confidence it had established. This will result in you receiving an informal reprimand which will not be explicitly referred to on your annual report, but may affect your immediate career advancement prospects, yet...

Not providing the information to others outside your work area will result in a significant and costly disruption to the implementation of a major project belonging to **another** Service.

(a) In this dilemma, how important do you think it is to maintain the confidence established by your work area? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(b) In this dilemma, how important do you think it is to provide the information to others outside your work area? *(please circle one number)*

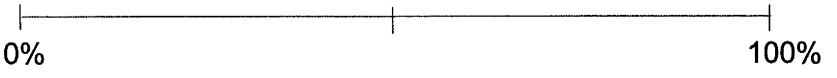
Not at all important 1 2 3 4 5 6 7 Very important

(c) What would you decide in this dilemma? *(please tick only one box)*

☐ I **would not** provide the information to others outside my work area

☐ I **would** provide the information to others outside my work area

(d) What percentage of peers from your Headquarters would you expect to decide *as you did* in this dilemma? *(please mark the line with an 'X' at any point)*



(e) How confident are you that your decision in this dilemma is the most appropriate decision? *(please circle one number)*

Not at all confident 1 2 3 4 5 6 7 Very confident

DILEMMA 8

Again, imagine yourself in **Scenario B** and you now face a dilemma where:-

Providing the information to others outside your work area will break the confidence it had established. This will result in you receiving an informal reprimand which will not be explicitly referred to on your annual report, but may affect your immediate career advancement prospects, yet...

Not providing the information to others outside your work area will lead to a situation in which certain strategic and operational areas of the ADF will be severely compromised in their ability to achieve key goals, and will likely lead to an increased risk of casualties to ADF personnel.

(a) In this dilemma, how important do you think it is to maintain the confidence established by your work area? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(b) In this dilemma, how important do you think it is to provide the information to others outside your work area? *(please circle one number)*

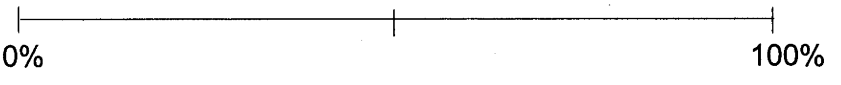
Not at all important 1 2 3 4 5 6 7 Very important

(c) What would you decide in this dilemma? *(please tick only one box)*

☐ I **would not** provide the information to others outside my work area

☐ I **would** provide the information to others outside my work area

(d) What percentage of peers from your Headquarters would you expect to decide *as you did* in this dilemma? *(please mark the line with an 'X' at any point)*



(e) How confident are you that your decision in this dilemma is the most appropriate decision? *(please circle one number)*

Not at all confident 1 2 3 4 5 6 7 Very confident

SCENARIO C

Scenario C below provides the backdrop to Dilemmas **9 - 12.**

In the course of your normal work duties you are privy to classified information about ADF activities. Upon receipt of official requests you provide this information to other areas of the ADF.

On this particular occasion, for reasons beyond your control, no time is available for an official request to be made and instead you have been asked to provide the information *unofficially*.

Assume that providing the information *unofficially* would not adversely affect any current or planned ADF operation.

DILEMMA 9

Imagine yourself in **Scenario C** and you now face a dilemma where:-

Providing the information unofficially will constitute a breach of national security and will lead to an investigation that will reveal *prima facie* commission of an offence under the Crimes Act, yet...

Not providing the information to those making the unofficial request will cause an ADF colleague from another work area within your Headquarters to make a bad decision that will unfairly limit their career advancement prospects.

(a) In this dilemma, how important do you think it is to **only** provide the information to those making an *official* request? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(b) In this dilemma, how important do you think it is to provide the information to those making the *unofficial* request? *(please circle one number)*

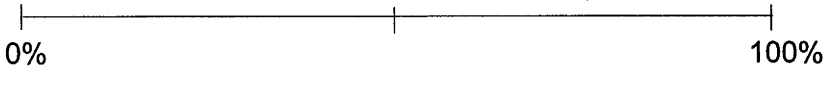
Not at all important 1 2 3 4 5 6 7 Very important

(c) What would you decide in this dilemma? *(please tick only one box)*

☐ I **would not** provide the information to those making unofficial requests

☐ I **would** provide the information to those making unofficial requests

(d) What percentage of peers from your Headquarters would you expect to decide *as you did* in this dilemma? *(please mark the line with an 'X' at any point)*



(e) How confident are you that your decision in this dilemma is the most appropriate decision? *(please circle one number)*

Not at all confident 1 2 3 4 5 6 7 Very confident

DILEMMA 10

Again, imagine yourself in **Scenario C** and you now face a dilemma where:-

> Providing the information unofficially will constitute a breach of national security and will lead to an investigation that will reveal *prima facie* commission of an offence under the Crimes Act, yet...
>
> Not providing the information to those making the unofficial request will result in a significant and costly disruption to the implementation of a major project belonging to **your** Service.

(a) In this dilemma, how important do you think it is to **only** provide the information to those making an *official* request? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(b) In this dilemma, how important do you think it is to provide the information to those making the *unofficial* request? *(please circle one number)*

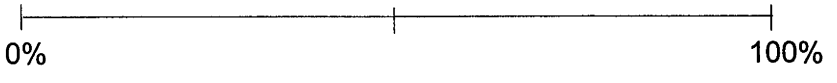
Not at all important 1 2 3 4 5 6 7 Very important

(c) What would you decide in this dilemma? *(please tick only one box)*

☐ I **would not** provide the information to those making unofficial requests

☐ I **would** provide the information to those making unofficial requests

(d) What percentage of peers from your Headquarters would you expect to decide *as you did* in this dilemma? *(please mark the line with an 'X' at any point)*



(e) How confident are you that your decision in this dilemma is the most appropriate decision? *(please circle one number)*

Not at all confident 1 2 3 4 5 6 7 Very confident

DILEMMA 11

Again, imagine yourself in **Scenario C** and you now face a dilemma where:-

> Providing the information unofficially will constitute a breach of national security and will lead to an investigation that will reveal *prima facie* commission of an offence under the Crimes Act, yet...
>
> Not providing the information to those making the unofficial request will result in a significant and costly disruption to the implementation of a major project belonging to **another** Service.

(a) In this dilemma, how important do you think it is to **only** provide the information to those making an *official* request? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(b) In this dilemma, how important do you think it is to provide the information to those making the *unofficial* request? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(c) What would you decide in this dilemma? *(please tick only one box)*

☐ I **would not** provide the information to those making unofficial requests

☐ I **would** provide the information to those making unofficial requests

(d) What percentage of peers from your Headquarters would you expect to decide *as you did* in this dilemma? *(please mark the line with an 'X' at any point)*

(e) How confident are you that your decision in this dilemma is the most appropriate decision? *(please circle one number)*

Not at all confident 1 2 3 4 5 6 7 Very confident

DILEMMA 12

Again, imagine yourself in **Scenario C** and you now face a dilemma where:-

> Providing the information unofficially will constitute a breach of national security and will lead to an investigation that will reveal *prima facie* commission of an offence under the Crimes Act, yet...
>
> Not providing the information to the unofficial request will lead to a situation in which certain strategic and operational areas of the ADF will be severely compromised in their ability to achieve key goals, and will likely lead to an increased risk of casualties to ADF personnel.

(a) In this dilemma, how important do you think it is to **only** provide the information to those making an *official* request? *(please circle one number)*

Not at all important 1 2 3 4 5 6 7 Very important

(b) In this dilemma, how important do you think it is to provide the information to those making the *unofficial* request? *(please circle one number)*

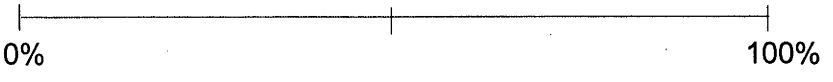
Not at all important 1 2 3 4 5 6 7 Very important

(c) What would you decide in this dilemma? *(please tick only one box)*

☐ I **would not** provide the information to those making unofficial requests

☐ I **would** provide the information to those making unofficial requests

(d) What percentage of peers from your Headquarters would you expect to decide *as you did* in this dilemma? *(please mark the line with an 'X' at any point)*



(e) How confident are you that your decision in this dilemma is the most appropriate decision? *(please circle one number)*

Not at all confident 1 2 3 4 5 6 7 Very confident

GENERAL ATTITUDES

Please indicate the extent to which you agree with the following statements:-
(please circle one number)

(a) I identify with my work area

Not at all 1 2 3 4 5 6 7 A great deal

(b) I identify with my Service

Not at all 1 2 3 4 5 6 7 A great deal

(c) I identify with the ADF as a whole

Not at all 1 2 3 4 5 6 7 A great deal

(d) I feel strong ties with the personnel of my work area

Not at all 1 2 3 4 5 6 7 A great deal

(e) I feel strong ties with the personnel of my Service

Not at all 1 2 3 4 5 6 7 A great deal

(f) I feel strong ties with the personnel of the ADF as a whole

Not at all 1 2 3 4 5 6 7 A great deal

(g) I am committed to the aims of my work area

Not at all 1 2 3 4 5 6 7 A great deal

(h) I am committed to the aims of my Service

Not at all 1 2 3 4 5 6 7 A great deal

(i) I am committed to the aims of the ADF as a whole

Not at all 1 2 3 4 5 6 7 A great deal

PARTICIPANT DETAILS

Again, as with all the information you have provided, your answers here are **entirely confidential** *(please tick where appropriate).*

1. What is your age? **< 25** ☐ **25-34** ☐ **35-44** ☐ **45-54** ☐ **> 55** ☐

2. What is your sex? **Male** ☐ **Female** ☐

3. What is your ADF rank?

Navy			
LCDR and below ☐	CMDR ☐	CAPT ☐	CDRE and above ☐
Army			
MAJ and below ☐	LTCOL ☐	COL ☐	BRIG and above ☐
Air Force			
SQNLDR and below ☐	WGCDR ☐	GPCAPT ☐	AIRCDRE and above ☐

4. To what level is your current ADO clearance?

UNCLASSIFIED to CONFIDENTIAL ☐ **SECRET** ☐ **TOP SECRET and above** ☐

5. For how long have you worked within the ADF?

0-5 yrs ☐ **5-10 yrs** ☐ **10-15 yrs** ☐

15-20 yrs ☐ **20-25yrs** ☐ **25+ yrs** ☐

Please provide any comments you may have overleaf.

Thank you for your participation.

COMMENTS:

APPENDIX B

DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION **DSTO**

This questionnaire continues a program of research that examines the knowledge environment of the Defence enterprise. It also forms part of a Ph.D being conducted at the Australian National University.

Your participation is **entirely voluntary**. **To ensure anonymity,** no personally identifying information (e.g., name, position) is requested. Hence, the results will not be reported (in any report or forum) in a way that identifies participants. The questionnaire should take **5 minutes** to complete.

The researcher is responsible for **secure storage** of completed questionnaires at the DSTO C3 Research Centre. Results will be made available to any participant upon request. If you have any questions relating to this research, please do not hesitate to contact me.

Derek Bopping
DSTO
derek.bopping@dsto.defence.gov.au 02-625-66226

INSTRUCTIONS

In this questionnaire, **a stated opinion** and **a short scenario** provide the backdrop to a number of questions.

Please respond to each question by circling the number that best represents your answer.

Comments are most welcome on the final page.

To begin, please respond to the following 3 statements by circling one number:

1. I identify with my Service.

1	2	3	4	5	6	7
Not at all						A great deal

2. I feel strong ties with the personnel of my Service.

1	2	3	4	5	6	7
Not at all						A great deal

3. I am committed to the aims of my Service.

1	2	3	4	5	6	7
Not at all						A great deal

There are several opinions held by members of the ADF about the issue of Jointness. The quote shown below reflects one of the most common opinions.

> "In the ADF, we work as a Joint team – a team where Jointness sets the standards, a team that knows Jointness is *inseparable* from *real* capability…
>
> The single-Service ethos is dead (or it should be dead). Retaining a 'single-Service mentality' is an excuse for not moving with the times. Ridding ourselves of single-Service traditions and replacing them with Joint values is the way to achieve responsiveness.
>
> …In Jointness, the potential of our forces is realised. Outdated ideas about 'single-Service loyalty' compromise that potential. Such loyalty has no relevance, as our future is Joint."

To what extent do you agree with the following statements:

1. I share this view of Jointness.

1	2	3	4	5	6	7
Not at all						Very much

2. This view of Jointness should be widely accepted by all members of the ADF.

1	2	3	4	5	6	7
Not at all						Very much

3. This view of Jointness is compatible with the traditions of my Service.

1	2	3	4	5	6	7
Not at all						Very much

4. This view of Jointness has been imported into the ADF from other military organizations (e.g., in Canada, U.S.).

1	2	3	4	5	6	7
Not at all						Very much

5. This view of Jointness is being pushed by some prominent parts of the ADF.

1	2	3	4	5	6	7
Not at all						Very much

There are several opinions held by members of the ADF about the issue of Jointness. The quote shown below reflects one of the most common opinions.

> "In the ADF we must work as a Joint team – one capable of integrating the unique abilities of each Service, one that can focus single-Service strengths into optimal capabilities.
>
> ...Our single-Service traditions are the building blocks of Jointness. They are, after all, highly relevant to Service ethos and performance. Complementing strong Service traditions and ethos with Joint concepts, where appropriate, is the way to achieve responsiveness.
>
> ...Jointness should not get in the way of the Services - it should help each Service to achieve the best overall outcomes."

To what extent do you agree with the following statements:

1. I share this view of Jointness.

1	2	3	4	5	6	7
Not at all						Very much

2. This view of Jointness should be widely accepted by all members of the ADF.

1	2	3	4	5	6	7
Not at all						Very much

3. This view of Jointness is compatible with the traditions of my Service.

1	2	3	4	5	6	7
Not at all						Very much

4. This view of Jointness has been imported into the ADF from other military organizations (e.g., in Canada, U.S.).

1	2	3	4	5	6	7
Not at all						Very much

5. This view of Jointness is being pushed by some prominent parts of the ADF.

1	2	3	4	5	6	7
Not at all						Very much

Please imagine the following scenario:-

You work in an Army Headquarters. As part of your usual work duties, you receive information about the readiness of certain force elements belonging to the Army.

On this occasion, you are one of several Army personnel privy to classified information that details a **temporary** lack of readiness of some force elements. The reasons for this lack of readiness would be clear to Army personnel, however this information could be interpreted by other personnel in a way that would **severely damage** the image of the Army.

Elsewhere, a Joint area is preparing a report on how the principles of Jointness can be used to improve the readiness of force elements.

We are interested in how you would respond to a **request** for the potentially damaging information from someone in the Joint area (that you don't know personally) who is either:-

(a) a cleared member of the **Army**; or

(b) a cleared member of **another Service**.

First, imagine the request comes from a cleared member of the Army:-

1. To what extent would you trust this individual not to allow the information to damage the image of the Army?

1	2	3	4	5	6	7
Not at all						Very much

How likely would you be to:

2. Provide the information to this individual immediately without further consultation?

1	2	3	4	5	6	7
Not at all						Very likely

3. Delay responding to this request in anticipation of a change in readiness circumstances?

1	2	3	4	5	6	7
Not at all						Very likely

4. Personally verify this individual's clearance and/or 'need-to-know'?

1	2	3	4	5	6	7
Not at all						Very likely

5. Seek advice from other Army personnel before deciding whether to provide the information to this individual?

1	2	3	4	5	6	7
Not at all						Very likely

6. Pass the responsibility for dealing with this request up the chain-of-command?

1	2	3	4	5	6	7
Not at all						Very likely

Please imagine the following scenario:-

You work in an Army Headquarters. As part of your usual work duties, you receive information about the readiness of certain force elements belonging to the Army.

On this occasion, you are one of several Army personnel privy to classified information that details a **temporary** lack of readiness of some force elements. The reasons for this lack of readiness would be clear to Army personnel, however this information could be interpreted by other personnel in a way that would **severely damage** the image of the Army.

Elsewhere, a Joint area is preparing plans for an imminent Joint operational deployment which may require those affected force elements.

We are interested in how you would respond to a **request** for the potentially damaging information from someone in the Joint area (that you don't know personally) who is either:-

(a) a cleared member of the **Army**; or
(b) a cleared member of **another Service**.

First, imagine the request comes from a cleared member of the Army:-

1. To what extent would you trust this individual not to allow the information to damage the image of the Army?

1	2	3	4	5	6	7
Not at all						Very much

How likely would you be to:

2. Provide the information to this individual immediately without further consultation?

1	2	3	4	5	6	7
Not at all						Very likely

3. Delay responding to this request in anticipation of a change in readiness circumstances?

1	2	3	4	5	6	7
Not at all						Very likely

4. Personally verify this individual's clearance and/or 'need-to-know'?

1	2	3	4	5	6	7
Not at all						Very likely

5. Seek advice from other Army personnel before deciding whether to provide the information to this individual?

1	2	3	4	5	6	7
Not at all						Very likely

6. Pass the responsibility for dealing with this request up the chain-of-command?

1	2	3	4	5	6	7
Not at all						Very likely

Now, imagine the request comes from a cleared member of another Service.

1. To what extent would you trust this individual not to allow the information to damage the image of the Army?

1	2	3	4	5	6	7
Not at all						Very much

How likely would you be to:

2. Provide the information to this individual immediately without further consultation?

1	2	3	4	5	6	7
Not at all						Very likely

3. Delay responding to this request in anticipation of a change in readiness circumstances?

1	2	3	4	5	6	7
Not at all						Very likely

4. Personally verify this individual's clearance or 'need-to-know'?

1	2	3	4	5	6	7
Not at all						Very likely

5. Seek advice from other Army personnel before deciding whether to provide the information to this individual?

1	2	3	4	5	6	7
Not at all						Very likely

6. Pass the responsibility for dealing with this request up the chain-of-command?

1	2	3	4	5	6	7
Not at all						Very likely

Finally,

7. If this information is **not provided** to anyone in the Joint area, how likely do you think it is that key ADF objectives will be compromised?

1	2	3	4	5	6	7
Not at all						Very likely

Demographics:- *(please tick where appropriate)*

Age:- _____ years

Sex:- ☐ Male ☐ Female

Rank:- ☐ **NCO** ☐ **2LT** to **CAPT** ☐ **MAJ** and above

Current ADO clearance:-

☐ Up to **CONFIDENTIAL** ☐ **SECRET** ☐ **TOP SECRET** and above

Years of Army service:- _____ years

Thank you for your participation **Comments are most welcome overleaf**

APPENDIX C

DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION **DSTO**

RESEARCH ON TRUST AND DISCLOSURE IN THE ADF.

This questionnaire is part of a program of research that examines the knowledge environment of the ADF. It also forms part of a PhD being conducted at the Australian National University.

Your participation is **entirely voluntary**. **No personally identifying information** (e.g., name, position) is requested. The questionnaire will take around **5 minutes** to complete.

Completed questionnaires will be stored securely at the DSTO C3 Research Centre, Canberra. Results will be made available to **any participant** upon request. For more information relating to this research, please do not hesitate to contact me:

Derek Bopping
Defence Science & Technology Organisation
Phone:02-625-66226
Email: derek.bopping@dsto.defence.gov.au

In this questionnaire, **a view of the RAN** and **a short scenario** provide the backdrop to a number of questions.

To begin, please indicate the extent to which you agree with the following 3 statements:
(circle one number)

1. I identify with the Royal Australian Navy.

1	2	3	4	5	6	7
Not at all						A great deal

2. I feel strong ties with Royal Australian Navy personnel.

1	2	3	4	5	6	7
Not at all						A great deal

3. I am committed to the aims of the Royal Australian Navy.

1	2	3	4	5	6	7
Not at all						A great deal

In the ADF, there are competing views of the Royal Australian Navy. One view that distinguishes 'supporters' of the Navy, is summarised below:

"...The Royal Australian Navy makes a first-rate contribution toward the defence of our national interests. The complexities of the maritime environment demand exceptional dedication, expertise, and dependability. The Navy has provided, and continues to provide these qualities to the ADF. It has built a reputation for excellence as a sea power that is underscored by its values of courage, integrity, and loyalty."

Please indicate below whether you share this view

☐ **Yes**, I share this view of the RAN. ☐ **No**, I do not share this view of the RAN.

... and respond to the following items:

I am confident that this view of the RAN truly captures my own personal beliefs.

1	2	3	4	5	6	7
Not at all						Very much

I see myself as a supporter of the RAN.

1	2	3	4	5	6	7
Not at all						Very much

We now want you to imagine a scenario that involves yourself and another member of the ADF (referred to as **'Person X'**). You will be asked 12 questions about how you would interact with Person X. To answer, you need to first consider the following points:

- Person X is a member of the RAN working on a report about ADF readiness.
- You know that Person X **is a supporter** of the RAN – that is, they genuinely hold the view of the RAN presented earlier.
- Person X asks you for classified information about the readiness of some RAN force elements (assume you're routinely privy to this information). Person X has the appropriate level security clearance.
- The information that Person X requests contains details about force elements being temporarily at unsatisfactory levels of readiness. The information could damage the image of the RAN if not managed with care.

Please turn the page...

In the ADF, there are competing views of the Royal Australian Navy. One view that distinguishes 'supporters' of the Navy, is summarised below:

"...The Royal Australian Navy makes a first-rate contribution toward the defence of our national interests. The complexities of the maritime environment demand exceptional dedication, expertise, and dependability. The Navy has provided, and continues to provide these qualities to the ADF. It has built a reputation for excellence as a sea power that is underscored by its values of courage, integrity, and loyalty."

Please indicate below whether you share this view

☐ **Yes**, I share this view of the RAN. ☐ **No**, I do not share this view of the RAN.

... and respond to the following items:

I am confident that this view of the RAN truly captures my own personal beliefs.

1	2	3	4	5	6	7
Not at all						Very much

I see myself as a supporter of the RAN.

1	2	3	4	5	6	7
Not at all						Very much

We now want you to imagine a scenario that involves yourself and another member of the ADF (referred to as **'Person X'**). You will be asked 12 questions about how you would interact with Person X. To answer, you need to first consider the following points:

- Person X belongs to one of the other Services, and is working on a report about ADF readiness.
- You know that Person X **is a supporter** of the RAN – that is, they genuinely hold the view of the RAN presented earlier.
- Person X asks you for classified information about the readiness of some RAN force elements (assume you're routinely privy to this information). Person X has the appropriate level security clearance.
- The information that Person X requests contains details about force elements being temporarily at unsatisfactory levels of readiness. The information could damage the image of the RAN if not managed with care.

Please turn the page...

In the ADF, there are competing views of the Royal Australian Navy. One view that distinguishes 'supporters' of the Navy, is summarised below:

"...The Royal Australian Navy makes a first-rate contribution toward the defence of our national interests. The complexities of the maritime environment demand exceptional dedication, expertise, and dependability. The Navy has provided, and continues to provide these qualities to the ADF. It has built a reputation for excellence as a sea power that is underscored by its values of courage, integrity, and loyalty."

Please indicate below whether you share this view

☐ **Yes**, I share this view of the RAN. ☐ **No**, I do not share this view of the RAN.

... and respond to the following items:

I am confident that this view of the RAN truly captures my own personal beliefs.

1	2	3	4	5	6	7
Not at all						Very much

I see myself as a supporter of the RAN.

1	2	3	4	5	6	7
Not at all						Very much

We now want you to imagine a scenario that involves yourself and another member of the ADF (referred to as **'Person X'**). You will be asked 12 questions about how you would interact with Person X. To answer, you need to first consider the following points:

- Person X is a member of the RAN working on a report about ADF readiness.
- You know that Person X **is not a supporter** of the RAN – that is, they genuinely do not hold the view of the RAN presented earlier.
- Person X asks you for classified information about the readiness of some RAN force elements (assume you're routinely privy to this information). Person X has the appropriate level security clearance.
- The information that Person X requests contains details about force elements being temporarily at unsatisfactory levels of readiness. The information could damage the image of the RAN if not managed with care.

Please turn the page...

In the ADF, there are competing views of the Royal Australian Navy. One view that distinguishes 'supporters' of the Navy, is summarised below:

"...The Royal Australian Navy makes a first-rate contribution toward the defence of our national interests. The complexities of the maritime environment demand exceptional dedication, expertise, and dependability. The Navy has provided, and continues to provide these qualities to the ADF. It has built a reputation for excellence as a sea power that is underscored by its values of courage, integrity, and loyalty."

Please indicate below whether you share this view

☐ **Yes**, I share this view of the RAN. ☐ **No**, I do not share this view of the RAN.

... and respond to the following items:

I am confident that this view of the RAN truly captures my own personal beliefs.

1	2	3	4	5	6	7
Not at all						Very much

I see myself as a supporter of the RAN.

1	2	3	4	5	6	7
Not at all						Very much

We now want you to imagine a scenario that involves yourself and another member of the ADF (referred to as **'Person X'**). You will be asked 12 questions about how you would interact with Person X. To answer, you need to first consider the following points:

- Person X belongs to one of the other Services, and is working on a report about ADF readiness.
- You know that Person X **is not a supporter** of the RAN – that is, they genuinely do not hold the view of the RAN presented earlier.
- Person X asks you for classified information about the readiness of some RAN force elements (assume you're routinely privy to this information). Person X has the appropriate level security clearance.
- The information that Person X requests contains details about force elements being temporarily at unsatisfactory levels of readiness. The information could damage the image of the RAN if not managed with care.

Please turn the page...

1. To what extent would you feel that Person X respected the Royal Australian Navy?

1	2	3	4	5	6	7
Not at all						A great deal

2. To what extent would you feel that you and Person X were "on the same side"?

1	2	3	4	5	6	7
Not at all						A great deal

3. To what extent would you feel that you and Person X were working toward a common goal?

1	2	3	4	5	6	7
Not at all						A great deal

4. How legitimate would you consider Person X's 'need to know' this information?

1	2	3	4	5	6	7
Not at all						Very legitimate

5. How confident would you be that Person X would manage this information with due care?

1	2	3	4	5	6	7
Not at all						Very confident

6. How important do you think it is that Person X obtain this information?

1	2	3	4	5	6	7
Not at all						Very important

How likely would you be to...

7. ...provide this information to Person X without further delay?

1	2	3	4	5	6	7
Not at all						Very likely

8. ...delay responding to Person X until the relevant readiness circumstances changed?

1	2	3	4	5	6	7
Not at all						Very likely

9. ...go to considerable lengths to verify Person X's security clearance?

1	2	3	4	5	6	7
Not at all						Very likely

10. ...seek advice from your Navy peers about how to deal with this request?

1	2	3	4	5	6	7
Not at all						Very likely

11. ...pass the responsibility for handling this request up the chain-of-command?

1	2	3	4	5	6	7
Not at all						Very likely

12. ...respect the concerns of Person X 'if the tables were turned'?

1	2	3	4	5	6	7
Not at all						Very likely

To finish, please complete the personal details section overleaf...

Personal details:

Age:- _____ years

Sex:- ☐ Male ☐ Female

Rank:- ☐ NCO ☐ ASLT to LEUT ☐ LCDR and above

Current ADO clearance:-

☐ Up to CONFIDENTIAL ☐ SECRET ☐ TOP SECRET and above

Years of RAN service:- _____ years

Thank you for your participation.

Any comments are most welcome below...

INTRUCTIONS

1. The aim of this questionnaire is to examine what ADF personnel think about the provision of classified information to each other.

2. On the next page, you will be asked to **rate how confident you would be** about a number issues involving the disclosure of classified information in the ADF. Each question requires that you respond **twice.**

That is, on the *left hand side* of the page, you are asked to respond keeping in mind disclosure that takes place **across Services**. See the example below (*do not complete*).

Example:

How confident would you be about being able to determine "need to know"?

*Disclosing **across** Services*						
1	**2**	**3**	**4**	**5**	**6**	**7**
Not at all confident						Very confident

And, on the *right hand side*, you are asked to respond to the same question, but this time keeping in mind disclosure that takes place **completely within your Service**:

*Disclosing **within** my Service*						
1	**2**	**3**	**4**	**5**	**6**	**7**
Not at all confident						Very confident

3. It is appreciated that, for some issues, your level of confidence will depend on many things (e.g., your experience) and that you would have more information in "real life" situations. However, we would appreciate if you would just try to indicate **your general level** of confidence towards the issues presented.

Please turn over...

How confident would you be...

(a) ...about being able to determine "need to know"?

*Disclosing **within** my Service*						
1	2	3	4	5	6	7
Not at all confident						Very confident

*Disclosing **across** Services*						
1	2	3	4	5	6	7
Not at all confident						Very confident

(b) ...about being able to anticipate or predict how the disclosed information might be used?

*Disclosing **within** my Service*						
1	2	3	4	5	6	7
Not at all confident						Very confident

*Disclosing **across** Services*						
1	2	3	4	5	6	7
Not at all confident						Very confident

(c) ...that any risks to your Service associated with disclosing will be **recognised** by the recipient(s)?

*Disclosing **within** my Service*						
1	2	3	4	5	6	7
Not at all confident						Very confident

*Disclosing **across** Services*						
1	2	3	4	5	6	7
Not at all confident						Very confident

(d) ...that any risks to your Service associated with disclosing will be **managed** by the recipient(s)?

*Disclosing **within** my Service*						
1	2	3	4	5	6	7
Not at all confident						Very confident

*Disclosing **across** Services*						
1	2	3	4	5	6	7
Not at all confident						Very confident

(e) ...that you **would not** be seen as "personally responsible" for disclosing classified information that ended up having a negative impact on the image of your Service.

*Disclosing **within** my Service*						
1	2	3	4	5	6	7
Not at all confident						Very confident

*Disclosing **across** Services*						
1	2	3	4	5	6	7
Not at all confident						Very confident

(f) ...about disclosing information about your Service to recipient(s) you do not know personally?

*Disclosing **within** my Service*						
1	2	3	4	5	6	7
Not at all confident						Very confident

*Disclosing **across** Services*						
1	2	3	4	5	6	7
Not at all confident						Very confident

To finish, please complete the personal details section overleaf...

Personal details:

Age:- _____ years

Sex:- ☐ Male ☐ Female

Rank:- ☐ NCO ☐ 2LT to CAPT (equivalents) ☐ MAJ and above (equivalents)

Current ADO clearance:-

☐ Up to CONFIDENTIAL ☐ SECRET ☐ TOP SECRET and above

Years of ADF service:- _____ years

Thank you for your participation.

Any comments are most welcome below.

APPENDIX E

RESEARCH ON DISCLOSURE IN THE ADF.

This questionnaire is part of a program of research that examines the knowledge environment of the ADF. It also forms part of a PhD being conducted at the Australian National University.

Your participation is **entirely voluntary. No personally identifying information** (e.g., name, position) is requested. The questionnaire will take around **5 minutes** to complete.

Completed questionnaires will be stored securely at the DSTO C3 Research Centre, Canberra. Results will be made available to **any participant** upon request. For more information relating to this research, please do not hesitate to contact:

Derek Bopping
Defence Science & Technology Organisation
Phone: 02-6125-0638
Email: derek.bopping@dsto.defence.gov.au derek.bopping@anu.edu.au

INTRUCTIONS

1. The aim of this questionnaire is to examine what ADF personnel think about the provision of classified information to each other.

2. To this end, a short scenario provides the backdrop to a number of questions.

3. Please read the scenario, then respond to the questions by circling the number that best represents you answer.

NOTE:

The scenario only provides "minimal" information. It is appreciated that in many "real-life" situations more information than that which is provided would be sought.

For the present purposes, please just try to indicate your **general** feeling when responding to the questions.

IMAGINE THAT:

You are routinely privy to classified information about the capability level of RAAF force elements as part of your normal duties.

On this occasion, you are approached by a member of the RAAF who is preparing a report concerning ADF preparedness. For the purposes of the report, this person (whom you don't know personally) requests that you provide classified information regarding the current capability level of certain RAAF force elements.

The information requested contains details about force elements being **temporarily at unsatisfactory levels of capability** and if not managed with care, could damage the image of the RAAF.

The requestor (who is appropriately cleared) **provides a guarantee** that you will be able to view the report before it is completed and disseminated.

Keeping this scenario in mind

1. To what extent would providing the information without delay be risking the RAAF's image?

1	2	3	4	5	6	7
Not at all						Very much

2. To what extent would providing the information without delay be risking your personal reputation?

1	2	3	4	5	6	7
Not at all						Very much

3. To what extent would you think the requestor has a 'need to know'?

1	2	3	4	5	6	7
Not at all						Very much

4. How confident would you be that the requestor would manage any risks to the image of the RAAF?

1	2	3	4	5	6	7
Not at all						Very confident

5. To what extent would you feel you could control how the requestor used the information?

1	2	3	4	5	6	7
Not at all						Very much

6. To what extent would you think it important that the requestor obtain the information?

1	2	3	4	5	6	7
Not at all						Very much

7. If you were to provide the information without delay, how confident would you feel that the final report would treat the RAAF fairly?

1	2	3	4	5	6	7
Not at all						Very confident

8. How likely would you be to provide the information to the requestor without delay?

1	2	3	4	5	6	7
Not at all						Very likely

IMAGINE THAT:

You are routinely privy to classified information about the capability level of RAAF force elements as part of your normal duties.

On this occasion, you are approached by a member of **another Service** who is preparing a report concerning ADF preparedness. For the purposes of the report, this person (whom you don't know personally) requests that you provide classified information regarding the current capability level of certain RAAF force elements.

The information requested contains details about force elements being **temporarily at unsatisfactory levels of capability** and if not managed with care, could damage the image of the RAAF.

The requestor (who is appropriately cleared) **provides a guarantee** that you will be able to view the report before it is completed and disseminated.

Keeping this scenario in mind

1. To what extent would providing the information without delay be risking the RAAF's mage?

1	2	3	4	5	6	7
Not at all						Very much

2. To what extent would providing the information without delay be risking your personal reputation?

1	2	3	4	5	6	7
Not at all						Very much

3. To what extent would you think the requestor has a 'need to know'?

1	2	3	4	5	6	7
Not at all						Very much

4. How confident would you be that the requestor would manage any risks to the image of the RAAF?

1	2	3	4	5	6	7
Not at all						Very confident

5. To what extent would you feel you could control how the requestor used the information?

1	2	3	4	5	6	7
Not at all						Very much

6. To what extent would you think it important that the requestor obtain the information?

1	2	3	4	5	6	7
Not at all						Very much

7. If you were to provide the information without delay, how confident would you feel that the final report would treat the RAAF fairly?

1	2	3	4	5	6	7
Not at all						Very confident

8. How likely would you be to provide the information to the requestor without delay?

1	2	3	4	5	6	7
Not at all						Very likely

IMAGINE THAT:

You are routinely privy to classified information about the capability level of RAAF force elements as part of your normal duties.

On this occasion, you are approached by a member of the RAAF who is preparing a report concerning ADF preparedness. For the purposes of the report, this person (whom you don't know personally) requests that you provide classified information regarding the current capability level of certain RAAF force elements.

The information requested contains details about force elements being **temporarily at unsatisfactory levels of capability** and if not managed with care, could damage the image of the RAAF.

The requestor (who is appropriately cleared) reminds you that **you will not** be able to view the report before it is completed and disseminated.

Keeping this scenario in mind

1. To what extent would providing the information without delay be risking the RAAF's image?

1	2	3	4	5	6	7
Not at all						Very much

2. To what extent would providing the information without delay be risking your personal reputation?

1	2	3	4	5	6	7
Not at all						Very much

3. To what extent would you think the requestor has a 'need to know'?

1	2	3	4	5	6	7
Not at all						Very much

4. How confident would you be that the requestor would manage any risks to the image of the RAAF?

1	2	3	4	5	6	7
Not at all						Very confident

5. To what extent would you feel you could control how the requestor used the information?

1	2	3	4	5	6	7
Not at all						Very much

6. To what extent would you think it important that the requestor obtain the information?

1	2	3	4	5	6	7
Not at all						Very much

7. If you were to provide the information without delay, how confident would you feel that the final report would treat the RAAF fairly?

1	2	3	4	5	6	7
Not at all						Very confident

8. How likely would you be to provide the information to the requestor without delay?

1	2	3	4	5	6	7
Not at all						Very likely

IMAGINE THAT:

You are routinely privy to classified information about the capability level of RAAF force elements as part of your normal duties.

On this occasion, you are approached by a member of **another Service** who is preparing a report concerning ADF preparedness. For the purposes of the report, this person (whom you don't know personally) requests that you provide classified information regarding the current capability level of certain RAAF force elements.

The information requested contains details about force elements being **temporarily at unsatisfactory levels of capability** and if not managed with care, could damage the image of the RAAF.

The requestor (who is appropriately cleared) reminds you that **you will not** be able to view the report before it is completed and disseminated.

Keeping this scenario in mind

1. To what extent would providing the information without delay be risking the RAAF's image?

1	2	3	4	5	6	7
Not at all						Very much

2. To what extent would providing the information without delay be risking your personal reputation?

1	2	3	4	5	6	7
Not at all						Very much

3. To what extent would you think the requestor has a 'need to know'?

1	2	3	4	5	6	7
Not at all						Very much

4. How confident would you be that the requestor would manage any risks to the image of the RAAF?

1	2	3	4	5	6	7
Not at all						Very confident

5. To what extent would you feel you could control how the requestor used the information?

1	2	3	4	5	6	7
Not at all						Very much

6. To what extent would you think it important that the requestor obtain the information?

1	2	3	4	5	6	7
Not at all						Very much

7. If you were to provide the information without delay, how confident would you feel that the final report would treat the RAAF fairly?

1	2	3	4	5	6	7
Not at all						Very confident

8. How likely would you be to provide the information to the requestor without delay?

1	2	3	4	5	6	7
Not at all						Very likely

Demographic details:

Age:- _____ years

Sex:- ☐ Male ☐ Female

Rank:- ☐ NCO ☐ PLTOFF to FLTLT ☐ SQNLDR and above

Current ADO clearance:-

☐ Up to CONFIDENTIAL ☐ SECRET ☐ TOP SECRET and above

Years of RAAF service:- _____ years

Thank you for your participation.

Any comments are most welcome below...